BEST: International Journal of Humanities,
Arts, Medicine and Sciences (BEST: IJHAMS)
ISSN (P): 2348-0521, ISSN (E): 2454-4728
Vol. 3, Issue 11, Nov 2015, 9-14
© BEST Journals

THREAT ON THE INTERNET—NEW ARENA OF CHALLENGES

M. V. CHANDRAMATHI[1] & B. SHREYAS GUPTA[2]

[1] Assistant professor, Symbiosis Law School, Hyderabad, India

[2] 3rd Year Student of Gitam Institute of Technology, Hyderabad, India

ABSTRACT

In recent years the convergence of religious fundamentalism and political activism has been a disturbing trend. Terrorists mostly target for most impact in conjunction of loss of life. However the terrorist first engages in targeting the violence against a country which is powerful and later it can be towards symbolic representation of technical advancement and power. Such instances are many to quote. Subsequently the terrorists targets towards technical advancement to endanger technical ability of a nation. Terrorist activities which is an innovation through implementation of technology by these terrorist in the age of information by giving it a new version—'techno -terrorism' and cyber terrorism. 'Cyber Terrorism' is the new form of terror that has to do more with 'information attacks' on a nation's computer system and information and infrastructure. Computers are the most modern crime contrivance today. The other testing legal question is when does internet activity involves *actus reus*.? it will prove difficult who had the thought first—the person or the machine.

Finally, the authors discuss the impact of this new dimension of cyber terrorism --has on the public at large and the governments in the way in which one should build one's defenses and counter this new dimension of cyber terrorism.

KEYWORDS: New Version—'Techno -Terrorism' and 'Cyber Terrorism', 'Information Attacks'

INTRODUCTION

Fear arises from inability to deal with physical pain and psychologically it is inability to deal with unknown such as loosing something such as darkness death etc., Living in fear becomes a psychological disease found in people who live under suppression, oppression and ignorance. Fear alters the natural behavior of a living creature to make him or her violent or attacking. We know that animals, (snakes, dogs etc.,) attack due to their own fear. This type violent attack spreads the disease of fear in the other who had no fear until then. Terror is the most violent expression of fear. Therefore it is conducted by those are in fear, or essentially cowards. Man may have become civilized, but the last three thousand years account for the political and religious polarization of this world by brute and violent force (born from psychological fear) and thus the world has progressively become a dangerous place to live in.

In recent years the convergence of religious fundamentalism and political activism has been a disturbing trend. Terrorists mostly target for most impact in conjunction of loss of life. However the terrorist first engages in targeting the violence against a country which is powerful and later it can be towards symbolic representation of technical advancement and power. Such instances are many. Next the terrorists targets towards technical advancement to endanger technical ability of a nation. This is a new dimension of terrorist activity which is done through implementation of technology by these terrorist in the age of information by giving it a new version—'techno -terrorism' and cyber terrorism.

‘Cyber Terrorism’ is the new form of terror that has to do more with ‘information attacks’ on a nation’s computer system and information and infrastructure. Computers are the most modern crime contrivance today.

Information technology (IT) has exposed the user to a huge data bank of information regarding everything and anything. However, it has also added a new dimension to terrorism. The possibility of such attacks in future cannot be denied. Terrorism related to cyber is popularly known as ‘cyber terrorism’.

In the age of information technology the terrorists have acquired a proficiency to bring into being the most fatal combination of weapons and technology which if not appropriately protected in due course of time, will take its toll. The damage so produced would be almost irreparable and mainly catastrophic in nature. In short we are facing the worst shape of terrorism popularly known as “cyber terrorism”. The phrase “cyber terrorism includes an intended harmful and harmful use of the information technology for producing harsh and damaging effects to the property, whether tangible or intangible of others. For instance, hacking of a computer system and then deleting the useful and priceless business information of the enemy challenger is a part and parcel of cyber terrorism.

THE CONCEPT OF CYBER TERRORISM

Before we can discuss the potential of “cyber terrorism” we must have some working definitions. The word “cyber terrorism” refers to two rudiments “cyber space” and “terrorism”. First of all any time the use of prefix cyber refers to something about moving fast. Movement is always drawn in. Anything associated to internet falls under the cyber category. Besides being a prefix, it is also a verb, not a noun. Therefore plugging in some 3D game and donning your goggles to go “cyber” doesn’t count. There is always action, inspiration, association and communication when you cyber, It’s not possible to just be cyber. There is no study state of being cyber. To cyber means that one is continuously moving across vast amounts of information, lots of information and one is persistently using technology to the max. It is commotion exclusive to the information or Knowledge Age we are entering, and by its very character, it involves several unique implications for changes in the approach we live.

The other testing legal question is when does internet activity involves *actus reus*? In cyber space, as in fundamental reality, it is the thought that what one is experiencing is factual. It does not necessitate tangible sensation to be practically raped in a chat room, but the penalty or trauma can be just as real. People can get married in cyber space; obtain college degrees, and so other things that have authentic consequences. Plagiarism and copyright violation is rampant on the web, and companies frequently install cookies and slot in, in data mining. A lot of internet content is unsuitable for children. Just how many crimes are possible to commit in cyber space is difficult to settle on, and prove some damaging action took place. Computer impersonation, symbols, and persons do not make for anything more than plot and budding offense charges. When AI (Artificial Intelligence) systems come online, it will prove difficult who had the thought first—the person or the machine.

Terrorist are known to use information technology to prepare plans, raise funds, spread misinformation, and communicate strongly. For example, Ramzi Yousef, architect of the first World Trade Center attack, stored comprehensive plans to demolish United States Airliners and encrypted files in his laptop computer. Osama Bin Laden was known to use steganography for his network’s connections. A website that was known as the Muslim Hacker’s club scheduled tips for things such as hacking the pentagon. A Hacker identified as DoctorNuker has been defacing websites with anti American, anti Israeli, and pro Bin Laden party line. Other than by using computers to exchange a few words and co-ordinate, few examples continue living of cyber terrorism or politically provoked attacks on computer system. In fact it is beneficial to a terrorist group to keep the internet working as a means of communiqué and outlet for propaganda. The chief paraphernalia of terrorism linger guns and bombs, not computers. There are a not many instances of cyber terrorism however such as the 1998 attack on Sri Lankan servers by the Internet Black Tigers or the Maxican Zapatista movement of the same year, which sooner or later teamed up with protesters of the World Trade Center. The world is yet to see a momentous instance of "cyber terrorism" with respect to wide spread disturbance of critical infrastructures. However, the FBI and many others anxious about the growth of the remarkable called hactivism, which is a word that combines hacking and activism. These are politically forced attacks, but they may also be a form of electronic civil defiance. Such attacks are usually stylish. For example, the Zapatistas targets the URL's of companies they think don't hold up human rights. The attack is nothing more than adding the phrase "human rights" to the end of the URL. The page precedes a display that says "human rights not found on this server." This is also set up in the server logs. They don't really flood the server, just sufficient times to make sure it is noticed in the server logs. Foreign Intelligence services have modified to using cyber tools as a part of their information congregation and spying tradecraft. In a case dubbed "the Cuckoo's Egg" between 1986 and 1989 a ring of West German hackers penetrated various military, scientific, and industry computers in the United States, Western Europe, and Japan, pilfering passwords, programmes and other information which they sold to the Soviet KGB, radically this was ancient history in Internet years.

Info warfare habitually involves foreign military forces against another foreign military force. We know that several nations are already on the increase information warfare doctrine, programs and capabilities for use in opposition to each other and the United States, China, Taiwan have been at info war for years. Foreign nations engrossed in such programmes feel they cannot overpower the United States in a head-to-head military encounter and consider that information technology is our Achilles Heel and their paramount bet.

FACETS OF CYBER TERRORISM

Who is a Hacker?

In computing, hacker has numerous meanings. People engaged in circumvention of computer security. This above all refers to unlawful remote computer break-ins via a communication network such as Internet.

In a safekeeping context, a hacker is someone involved in computer security/insecurity, specializing in the detection of exploits in systems (for exploitation or prevention), or in obtaining or preventing unlawful access to systems from end to end skills, tactics and thorough knowledge. In the most widespread general form of this usage, "hacker" refers to a black-hat hacker (a malicious or criminal hacker). There are also moral hackers (more commonly referred to as white hats), and those more ethically ambiguous (grey hats). To disambiguate the term hacker, often cracker is used as an alternative, referring what's more to computer security hacker culture as a whole to differentiate it from the academic hacker ethnicity or specifically to make a difference within the computer security framework between black-hat hackers and the more ethically positive hackers (commonly known as the white-hat hackers). The outlook of computer defense hacking forms a subculture which is often referred to as a network hacker subculture or simply the computer dissident

Case Studies of Hackers

- 1972,: Capt. Crunch" aka John Draper, realized that by blowing the whistle that came in Capt. Crunch cereal boxes, he could reproduce the tones necessary to place free long distance phone calls. He spent some time on probation and in prison, and then went to work with Apple Computer.[1]

- In 1994, Mitnick was the worlds' most wanted hacker for hacking the Digital Equipment's Computers and pilfering source codes. He spent few years in prison and later became a book author.[2]
- In 1995 Poulsen, a friend of Mitnick bust into FBI computers. He spent some time in prison and later happens to be a Computer Security Journalist.[3]
- Onel DeGuzman was a Philippine computer science student who unleashed the "I LOVE YOU" virus on the internet. He was not punished because Philippine State had no law covering such a crime then.[4]

INDIAN CASES OF HACKERS

- On 6th February 2001, Delhi police arrested two hackers. This became breaking news in India. They hacked a website. This was the first case in India where the accused were arrested.[5]
- On 5th July 2001 the Cyber Crimes Investigation Cell Mumbai acknowledged an unknown telephone at about 07:00 PM that their website www.ccicmumbai.com is going to be attacked by hackers. Instantaneously Police Officers noticed that it has been hacked.
- In The Year 2001, one Ex-Scientist was arrested from ISRO for E-mail threats to the Department of Atomic Energy and hacking of an Internet Service Provider, Ice net at Ahmadabad; India and also for sending e-mails treat to the nations security which is also to be treated as cyber terrorism.[6]

Cyber Terrorist Prefer using the Cyber Attack Methods because of Many Advantages

- It is cheaper than any of the traditional methods.
- The action is very difficult to be traced.
- It is easy to conceal themselves and their location.
- There can no bodily barriers.
- They can impinge on a big number of people.

INSTANCES OF CYBER TERRORISM

In 1998, ethnic Tamil guerrillas flooded Sri Lankan embassies with 800 e-mails a day over a two-week period[7]. The messages read "We are the Internet Black Tigers and we're doing this to disrupt your communications." Intelligence authorities characterized it as the first known attack by terrorists against a country's computer systems.

During the Kosovo conflict in 1999, NATO computers were blasted with e-mail bombs and hit with

[1] http://maryamheidari.blogspot.in/
[2] ibid
[3] Ibid supra
[4] http://www.teachingterror.com/syllabi/315lect12.htm
[5] http://ncdrc.res.in/press-and-media-centre/case-studies/
[6] Ibid
[7] http://maryamheidari.blogspot.in/

denial-of –service attacks by hacktivists protesting the NATO bombings[8]. In addition, businesses, public organizations, and academic institutes received greatly politicized virus-laden e-mails from a range of Eastern European Countries, according to reports. Web defacements were also widespread.

Since December 1997, the Electronic Disturbances Theater (EDT) has been conducting Web sit-ins against various sites in support of the Mexican Zapatistas. At a designated time, thousands of protesters point their browsers to a target site using software that floods the target with rapid and repeated download requests. EDT's software has also been used by animal rights groups against organizations said to abuse animals.

To make the grade as cyber terrorism attacks or intimidation of attacks must result in violence against people or property or must produce considerable fear of violence. Terrorism in cyberspace can take many diverse forms: physical destruction of machinery crucial to an IT infrastructure, remote intervention of computer networks, interruption of government networks, or even interruption of societal networks such as financial networks or mass media. Even such acts as data fraud and website defacement can be considered cyber terrorism if the effect was intentional pervasive damage and violent behavior to people or property.

Visualizing, if a terrorist organization were to expand information regarding the government's nuclear weapons, right to use and use of such information could have fatal and lasting consequences. The answer is the actual use of this information. Imagine if someone were to learn the science in the wake of nuclear arsenal and how to manufacture a nuclear bomb. This information alone is not dangerous; however if the awareness is used by one with malicious intent then it can be shocking. Consider about a terrorist organization structure a nuclear weapon and using it within the United States. Not merely will thousands, perhaps even millions, suffer fatality, but that area affected may not be able to uphold any form of life. If this same information was obtained by a world renowned scientist and was used to enhance world security aligned with malicious intent, then it would be a great contribution to the global society. Such issues of security are all dependent on how the information is used.

Indian Challenges and Concerns in the Arena of Cyber Space

There are too many challenges and concerns in the arena of cyber space.

- Lack of awareness at the citizen level and at the institutional level too.
- Lack of skilled and competent manpower to execute the counter measures.
- Many information security organizations have turned to be feeble for the reason of 'turf wars'.
- Lack of e-mail account policy for most essential National Services like Defence Forces and the Police.
- The cyber threats are not only from terrorist organization but also from neighboring countries that are hostile to our National Interests.

CONCLUSIONS AND RECOMMENDATIONS

Recommendations

- Call to sensitize the citizens regarding the dangers encountered due to cyber terrorism.

[8] "Hackers attack U.S. government Web sites in protest of Chinese embassy bombing". *CNN*. Retrieved 2010-04-30.(See also Chinese embassy bombing)

- Call for qualified and skilled personnel form understanding and implementation of counter procedures by the governmental agencies and the defence forces.
- Support of the cyber security must not merely be a lip service.
- Cyber security Agreements are to be given the same importance as that of other conventional agreements.
- Government must provide more budget and manpower for Cyber security.
- Cyber Security is too keep more vigil over the developments in the field of Information Technology Segment of our probable adversaries.

CONCLUSIONS

The need of the hour has come where it has become necessary to prioritize cyber security into India’s counter terrorism strategy. There is a growing association between the hacker and the terrorist that which could result in the terrorist themselves would grow to be excellent hackers. This could change the entire backdrop of terrorism. The world is challenged with this problem and are effectively trying to curb it. This is possible only by the support of the public and a vigilant government. The legislature cannot make legislations which are against public opinion and public policy. Therefore the public support is necessary.

Citizens are conscious about their legitimate rights and the law has to be enacted taking care of the public interest on a precedence basis. This can be achieved through suitable technology backed by the support of appropriate legislation which must be exclusive regarding the menace of the malware which are created by the computers sending it. India has fortunately a sound legal pedestal for dealing with malware and the general public has no problem to support the self-help procedures to combat cyber terrorism and malwares.

REFERENCES

1. http://maryamheidari.blogspot.in/
2. http://www.teachingterror.com/syllabi/315lect12.htm
3. http://ncdrc.res.in/press-and-media-centre/case-studies/
4. http://maryamheidari.blogspot.in/
5. "Hackers attack U.S. government Web sites in protest of Chinese embassy bombing". *CNN.* Retrieved 2010-04-30.(See also Chinese embassy bombing.
6. Cyber Terrorism By Kevin Coleman, Technolytics.
7. Cybercrime and cyberterrorism: Preventive defense for cyberspace violations By PRAVEEN DALAL
8. Coleman, Keivin "Cyber Terrorism"
9. Collin, Barry C. "The Future of Cyber Terrorism"