Quest Journals
Journal of Research in Humanities and Social Science
Volume 5 ~ Issue 4 (2017) pp: 27-30
ISSN(Online) : 2321-9467
www.questjournals.org

Research Paper

A Biggest Threat to India – Cyber Terrorism and Crime

Smt. Saheli Naik
Assistant Professor Of Political Science, Kabi Sukanta Mahavidyalaya, Bhadreswar, Hooghly, West Bengal, India.

Received 08 Apr, 2017; **A**ccepted 20 Apr, 2017 © The author(s) 2017. **P**ublished with open access at **www.questjournals.org**

I. INTRODUCTION

The threat of terrorism has posed an immense challenge in our everyday life. Terror attacks in major cities, towns and tourist resorts across the globe have demonstrated the inadequacy of the state mechanism to address the challenge. The nations are attains many major counter strategies to cope up the challenges. However, most of the attempts are designed as conventional method which might be effective in conventional terror attacks. However, there are limitations when it comes to a terror attack of an unconventional nature. have demonstrated the inadequacy of the state mechanism to address the challenge. The nations are attains many major counter strategies to cope up the challenges. However, most of the attempts are designed as conventional method which might be effective in conventional terror attacks. However, there are limitations when it comes to a terror attack of an unconventional nature.

Information technology (IT) has exposed the user to huge data bank of information about everything and anything. However, it has also added a new dimension to terrorism. Recent reports tells us the terrorist is also getting equipped to utilize the cyber space to carry out terror attacks. The possibility of such attacks in future cannot be denied. Terrorism related to cyber space is popularly known as "cyber terrorism".

In the last couple of decades India has carved a niche for itself in IT. Most of the Indian Banking Industry, Post Offices, Other Offices, Financial Institutions have introduced IT replacing manual process. The cyber terrorist attacks are mainly occurred in these institutions through IT i.e: hacking, fraud e-mails, ATM hacking, cell phones, satelite phone hacking etc... i.e: hacking, fraud e-mails, ATM hacking, cell phones, satelite phone hacking etc...

The article envisages and understanding of the nature and effectiveness of cyber attacks and making an effort to study and analyze the efforts made by India to address the challenge and highlight what more could be done.

Thus articles is structured as given below:
1. Definition of cyber terrorism and cyber crime
2. Method of attacks
3. Tools of attacks
4. How Indian national security is affected by cyber terrorism and cyber attacks
5. Existing cyber security initiative
6. Our concerns
7. Some recommendations
8. Conclusions

1. Definition of cyber terrorism and cyber crime

Cyber crime is a crime related to computer and computer technology. The computer may have been used in a commission of a crime or it may be a target. Cyber crimes may affects a country's national security and financial condition. The types of crime are hacking, copyright infringement, child pornography and child grooming[1] . In this aspect, individual may be affected by disclosing their confidential matters like ATM Pin, Bank Details etc.. in open place. A nation-state will be attacked when some terrorist groups are mailing about women security, cross border crimes, financial theft etc...

Prof. Debararti Halder and Prof. K. Jaishankar defined cyber crimes as "offenses that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of victim or cause physical or mental harm or loss to the victim directly or indirectly using modern telecommunication networks such as Internet and Mobile Phones(SMS/MMS)"[2]. This two anthers also commented of perspective gender and defined cyber crime against women as "crimes target against women with a motive to intentionally harm the victim psychologically and physically using modern telecommunication networks such as Internet and Mobile Phones "[3].

Cyber terrorism is the act of internet terrorism in terrorist activities. Cyber terrorism is a controversial term. Some authors chose a very narrow meaning. They think that this terrorism is related to deployment, by known terrorist organization, or disruption attacks against information systems for the primary purpose of creating alarm and panic. Other authors chose a much broad definition which tends to falsely include cyber crime when its reality, they think that the cyber

crime and cyber terrorism two different issues[4] . Cyber terrorism can also be defined at the intentional use of computer, networks and public internet to cause destruction and harm for personal objectives[5]. The objective of these terrorists may be political or ideological since this can be seen as a form of terrorism. The objective of these terrorists may be political or ideological since this can be seen as a form of terrorism.

This terrorist organizations are like Alqaeda, ISIS, Mujahidines etc... These groups use the internet to communicate their members. Eugene Kaspersky now feels that cyber terrorism is a more accurate term than cyber war[6]. He stated that "without attacks they are clueless who did it or when they will strike again so it's not a cyber war but a cyber terrorism"[7]. Some authors say that cyber terrorism does not exist and is readily a matter of hacking or information warfare [8].

In a broad way cyber terrorism is defined as "The premeditated use of disruptive activities or the threat thereof, against computers and networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives " religious, political or similar objectives "[9]. The term appears first in the defense literature, surfacing in reports by US Army War College as early as 1998. The national conference of state legislator and organization of legislator created to help policy makers with issues such as economy and homeland security defined cyber terrorism as "The use of information technology by terrorist groups and individuals to further their agenda. This can include IT to organize and execute attacks against networks, computer systems and telecommunications, infrastructures or for exchanging information or making threats electronically."[10].

II. Method Of Attacks

The most popular weapon in cyber terrorism is computer viruses and warms. So this terrorism is also known as computer terrorism. The attacks or methods on the computer infrastructure can be classified into three different categories[11].

a. Physical Attack:

The computer infrastructure is damaged by using conventional methods by this attacks like bomb, fire etc...

b. Syntactic Attack:

The computer infrastructure is damaged by modifying the logic of the system in order to introduce delay or make the system unpredictable computer viruses and trojans are used in this type of attacks. computer viruses and trojans are used in this type of attacks.

c. Semantic Attack:

This is more damaging where it exploits the confidence of the user in the system. During this attack the information keyed in the system during entering and existing the system is modified without a user's knowledge.

One of the research community 'Tripwire' was published their article named - "Where are your cyber attacks coming from?" in Verizon's DBIR 2015. They explain that the five most common attack patterns of 2014 of the cyber attack. The attack types were 2015. They explain that the five most common attack patterns of 2014 of the cyber attack. The attack types were [12].

- Web Application : The authors of DBIR 2015 were noticed that organized crime has become the most frequently seen actor behind web application attacks.
- Privilege Misuse : This attacks are happened for financial gain.
- Cyber Espionage : Manufacturing, public and professional industries were most affected by this.
- Crimeware
- Point Of Sale

III. TOOLS OF ATTACK

Cyber terrorists use certain tools and methods to unleash this new age of terrorism. The tools of attacks are [13]

- **Hacking :** It is the most popular way used by a terrorist. It is a generic term used for any kind of unauthorized access to a computer. Hacking are related to packets snipping, tempest attack, password cracking etc...
- **Trozans :** Programs which pretend to do one thing while actually they are meant for doing something different, like the wooden trozan horse of the 12th century BC.
- Emails: Somewhere viruses and warms are attached themselves to a host program to be injected. Emails are used for spreading disinformation, threats and defamatory stuff.
- Computer virus and warms : A computer virus is a type of malicious software program ("malware") that, when executed, replicates by reproducing itself (copying its own source code) or infecting other computer programs by modifying them.[14] The computer warm is a term related to computers which is a self contained programming or a set off programs i.e able to spread functional copies of itself. able to spread functional copies of itself.

IV. HOW INDIAN NATIONAL SECURITY IS AFFECTED BY CYBER TERRORISM AND CYBER ATTACKS

India started to use information technology in many public sectors like Income Tax, Passport Service, Bank, Visa etc.... in terms of e-governance. Sectors like police and judiciary are to follow. The travel sector is also heavily reliant on this. Full computerization in this sector has also brought in concept of e-commerce. To create havoc in the country these are very lucrative targets to paralyze the economic and financial institutions. information technology in many public sectors like Income Tax, Passport Service, Bank, Visa etc.... in terms of e-governance. Sectors like police and judiciary are to follow. The travel sector is also heavily reliant on this. Full computerization in this sector has also brought in concept of e-commerce. To create havoc in the country these are very lucrative targets to paralyze the economic and financial institutions.

Mumbai terrorist attack on November, 2008 forced India to take military action against Pakistan. In response, Pakistan Government also was developing tactical nuclear weapon at a rapid pace. Those measures created deterrent between two countries. on November, 2008 forced India to take military action against Pakistan. In response, Pakistan Government also was developing tactical nuclear weapon at a rapid pace. Those measures created deterrent between two countries.

In March, 2013, Defense Research and Development Organization (DRDO) suspected that the chinse hackers breached the computers of India's top military organizations. After that India's defense minister at that time A.K. Antony ordered for the proof of the matter though an official statement denied any sensitive file had been compromized[15]. According to Supreme Court lawyer and leading cyber law expert Pavan Duggal while the threat of cyber attacks remain "imminent", the country lacks an institutionalist mechanism of the cyber army to deal with the threat. He also told that cyber warfare as a phenomenon is not covered under the Indian cyber laws as a phenomenon is not covered under the Indian cyber laws[16]. Over the past few years, India had witnessed a growing numbers of cyber assault with government departments. DRDO also confirmed that some hackers from Algeria also carried out an attack on websites run by DRDO, PMO and other various governmental offices.

According to CERT-in which is a government mandate information technology security organization estimated 14392 websites in the country were hacked in 2012, a report told that in 2011 as many as 14232 websites were hacked while the number of websites were hacked in 2009 stood at 9180 and in 2010, it was 16126[17]. Rikshit Tandon, consultant and internet and mobile association of India (IAMAI)and adviser to the cyber crime unit of UP police said that cyber terrorism was a grave threat not only to India but also to world[18]. A report also told that about 90119369 indian websites were hacked from 2012 to 2015. Most of them were governmental offices, defense sector , diplomatic missions, railways, bsnl, TRAI, CBI etc... In EC council report tells us that talent crisis in Indian information security, revealed that a major gaps in present day skill situation concerning IT security which can impact handling of cyber threats in industries such as banking, defense, healthcare, information technology, energy etc... EC also unveiled that about 75% of the participants showcased low level or a lack of skill in error handling, thereby displaying vulnerability known to lead to disclosure of sensitive information and denial of service attacks[19].

Indian home minister Rajnath Singh described that cyber terrorism as one of the biggest threat to the society along with cyber crime. Addressing the Indian Police Services (IPS) officers trainees of 2015 batch who came to meet him. At that time, Singh said that cyber crime becomes a challenge and it is being faced by the police these days. In his language cyber crime of the cyber world can be multilayered, multilocation, multilingual, multicultural and multilegal so it is difficult to investigate and reach to the criminal[20]. He also told that the officers should work with zeal towards the problem of people. The home minister also appealed to the officers to attain higher standards of excellence along with professional standards by integrating technology aspects of intelligence, surveillance, communications and modern policing[21].

In a public news paper, Indian Express news tells us that after the Narendra Modi government's historic "currency banned effect" between December 9 to 12, 2016 at least 80000 cyber attacks targeted to indian networks, showing that "why the government attempt to switch over to a digital economy". Top intelligence sources says that till November 28, 2016 they had observed and average 2 lacs threat and vulnerabilities per day. These increased to 5 lacs after the note ban issue and it further went up to 6 lacs threats by the first week of december[22]. The banking sector threats are increasing and they ordered for 360 degree security audit of information infrastructure including financial networks. An intelligence note reviewed by Indian Express once against the vulnerabilities of mobile phones The banking sector threats are increasing and they ordered for 360 degree security audit of information infrastructure including financial networks. An intelligence note reviewed by Indian Express once against the vulnerabilities of mobile phones[23]. A sources said that between November 22 and 26, 2016, we observed 335000 attacks in indian networks by hackers from China, Pakistan, Singapore, USA, Russia, Romania, Ukrane, Dubai, Sweden. In October, 2016, 3200000 debit cards issued by SBI, HDFC bank, ICICI bank AXIS bank, Yes bank were compromised in the largest yet cyber attack on the indian banking system.

V. EXISTING CYBER SECURITY INITIATIVE

To cope up the cyber crime and cyber terrorism India used her security program. Some organization incorporated to Police, I.B. DEPARTMENT started to collect their information world-wide. Here is some examples:

- National Information Centre (NIC) : Its an organization providing network backbone and e-governance support to the Central Govt., State Govt., Indian territories, districts and Govt. bodies.
- Indian Computer Emergency Response Team (CERT-IN) : It is the most important organization in India's cyber community initiative groups. Its mandate states that to ensure security of cyber space in a country by enhancing the security communication and information infrastructure.
- National Information Security Assurance Program (NISAP) : This is for Govt. and critical infrastructures. This Govt. organizaion used security policy and create a point of contact for the Govt. and critical infrastructure. This is a governmental organization creation by CERT-IN.
- The National Association Of Software And Services Companies (NASSCOM) : The National Association of Software and Services Companies (NASSCOM) is a trade association of Indian Information Technology (IT) and Business Process Outsourcing (BPO) industry. Established in 1988, NASSCOM is a non-profit organization. NASSCOM role has primarily related to software services or BPO services, its an organization to make sure that service quality and enforcement of intellectual property rights have been properly implemented in the Indians Software and BPO industry.

VI. OUR CONCERNS

Its a big concern to us that most of the Indian citizen does not know how to use modern technology at all. Lack of awareness and culture of cyber security at individual as well as institutional level. India does not have trained and qualified

man power to increment the counter measures. There is a big concern in lack of strong IT act in India and the cyber laws are also old. There is no email account policy for the defense forces, police and other institutional levels in the country.

VII. SOME RECOMMENDATIONS

Some recommendations are given below:

- Need to sensitize the common citizen about a danger of cyber terrorism. CRT-IN should engage academic institutions and follow an aggressive strategy
- Join efforts by all Govt. agencies including defense forces to attract qualified, skilled personal for implementation of counter measures
- More investment in this field
- Govt. law and IT act need to be rectified
- Need to have more international collaboration in the field of cyber security and favours handling issue of cyber terrorism in cooperation with other countries

VIII. CONCLUSIONS

There is a growing nexus between the hackers and terrorists. 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. Warren G. Kruse, Jay G. Heiser (2002). Computer forensics: incident response essentials. Addison-Wesley. p. 392. ISBN 0-201-70719-5.
2. 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
3. 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
4. Hower, Sara; Uradnik, Kathleen (2011). Cyberterrorism (1st ed.). Santa Barbara, CA: Greenwood. pp. 140–149. Retrieved 4 December 2016.
5. Matusitz, Jonathan (April 2005). "Cyberterrorism:". American Foreign Policy Interests. 2: 137–147.
6. "Latest viruses could mean 'end of world as we know it,' says man who discovered Flame", The Times of Israel, June 6, 2012
7. "Latest viruses could mean 'end of world as we know it,' says man who discovered Flame", The Times of Israel, June 6, 2012
8. Harper, Jim. "There's no such thing as cyber terrorism". RT. Retrieved 5 November 2012.
9. http://oai.dtic.mil/oai/oai?&verb=getRecord&metadataPrefix=html&identifier=ADA439217 as accessed on 08th April, 2017
10. Cyberterrorism National Conference of State Legislatures.https://en.wikipedia.org/wiki/Cyberterrorism, as accessed on 08th April, 2017
11. https://en.wikipedia.org/wiki/Cyber-attack as accessed on 08th April, 2017
12. https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-5-most-common-attack-patterns-of-2014/ as accessed on 08th April, 2017
13. http://ids.nic.in/art_by_offids/Cyber%20security%20in%20india%20by%20Col%20SS%20Raghav.pdf as accessed on 08th April, 2017
14. http://ids.nic.in/art_by_offids/Cyber%20security%20in%20india%20by%20Col%20SS%20Raghav.pdf as accessed on 08th April, 2017
15. Defence Minister AK Antony should have apologised, says LK Advani - http://www.ndtv.com/india-news/defence-minister-ak-antony-should-have-apologised-says-lk-advani-531573 as accessed on 08th April, 2017
16. India must wake up to cyber-terrorism http://gadgets.ndtv.com/internet/news/india-must-wake-up-to-cyber-terrorism-349274 as accessed on 8th April, 2017
17. Cyber defence: How prepared is India for cyber warfare - http://economictimes.indiatimes.com/tech/internet/cyber-defence-how-prepared-is-india-for-cyber-warfare/articleshow/19152928.cms as accessed on 8th April, 2017
18. India must wake up to cyber-terrorism - http://gadgets.ndtv.com/internet/news/india-must-wake-up-to-cyber-terrorism-349274 as accessed on 8th April, 2017
19. India not prepared to handle cyber terrorism threat:EC Council http://www.business-standard.com/article/pti-stories/india-not-prepared-to-handle-cyber-terrorism-threat-ec-council-114021900965_1.html as accessed on 8th April, 2017
20. Cyber terrorism biggest threat: Rajnath Singh http://www.india.com/news/india/cyber-terrorism-biggest-threat-rajnath-singh-1653594/ - as accessed on 8th April, 2017
21. Cyber terrorism biggest threat: Rajnath Singh http://www.india.com/news/india/cyber-terrorism-biggest-threat-rajnath-singh-1653594/ - as accessed on 8th April, 2017
22. 80,000 cyber attacks on December 9 and 12 after note ban http://www.newindianexpress.com/nation/2016/dec/19/80000-cyber-attacks-on-december-9-and-12-after-note-ban-1550803.html as accessed on 8th April, 2017
23. 80,000 cyber attacks on December 9 and 12 after note ban http://www.newindianexpress.com/nation/2016/dec/19/80000-cyber-attacks-on-december-9-and-12-after-note-ban-1550803.html as accessed on 8th April, 2017