

CYBER SECURITY IN INDIA'S COUNTER TERRORISM STRATEGY

Introduction

1. The threat of terrorism has posed an immense challenge in the post Cold War period. Terror attacks in major cities, towns and tourist resorts across the globe have demonstrated the inadequacy of the State mechanisms to address this challenge. Serious attempts have been made by Nations to address this challenge by designing counter terrorism strategies and anti terror mechanisms. However, most of these are designed in a conventional paradigm, which might be effective in a conventional terror attack. However, there are limitations when it comes to a terror attack of an unconventional nature.

2. 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. Recent reports suggest that the terrorist is also getting equipped to utilize cyber space to carryout terrorist attacks. The possibility of such attacks in future cannot be denied. Terrorism related to cyber is popularly known as 'cyber terrorism'.

3. In the last couple of decades India has carved a niche for itself in IT. Most of the Indian banking industry and financial institutions have embraced IT to its full optimization. Reports suggest that cyber attacks are understandably directed toward economic and financial institutions. Given the increasing dependency of the Indian economic and financial institutions on IT, a cyber attack against them might lead to an irreparable collapse of our economic structures. And the most frightening thought is the ineffectiveness of reciprocal arrangements or the absence of alternatives.

4. The article envisages an understanding of the nature and effectiveness of cyber attacks and making an effort to study and analyse the efforts made by India to address this challenge and highlight what more could be done. The article is structured as given below :-

- (a) Definition of Cyber Terrorism.
- (b) Methods of Attack.
- (c) Tools of Cyber Terrorism.
- (d) Challenges to India's National Security.
- (e) Existing Cyber Security Initiatives.
- (f) Challenges and Concerns.
- (g) Recommendations.

Definition of Cyber Terrorism

5. As the Nation became successful in unearthing terrorist networks involved in the recently carried out terror attacks, the most outstanding feature was the use of the tools of the information age like emails, cell phones, satellite phones etc to stay connected. The worrying aspect was the use of modern gadgets bringing out that the terrorist is not only obsessed with IEDs and AK-47 but has also mastered the use of laptops and tablet PCs to give finesse to his nefarious designs. As terrorist organizations realize its capability and

potential for disruptive efforts at lower costs they will become more and more technology savvy and their strategies and tactics will have a technological orientation.

6. One of the definitions of cyber terrorism states that :-

'Cyber terrorism is the convergence of terrorism and cyber space. It is generally understood to mean unlawful attacks and threats of attacks against computers, networks, and information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber terrorism, an attack should result in violence against persons or property or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber terrorism depending upon their impact. Attacks that disrupt non essential services or that are mainly a costly nuisance would not'

7. This is one of the most comprehensive definitions of cyber terrorism. But even this has a limitation. It states that for an attack to qualify as a cyber attack it should lead to violence. This is more conventional. Terrorist may direct an attack only to disrupt key services. If they create panic by attacking critical systems/infrastructure there is no need for it to lead to violence. In fact such attacks can be more dangerous.

Methods of Attacks

8. The most popular weapon in cyber terrorism is the use of computer viruses and worms. That is why in some cases of cyber terrorism is also called 'computer terrorism'. The attacks or methods on the computer infrastructure can be classified into three different categories.

(a) Physical Attack. The computer infrastructure is damaged by using conventional methods like bombs, 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 attack.

(c) Semantic Attack. This is more treacherous as it exploits the confidence of the user in the system. During the attack the information keyed in the system during entering and exiting the system is modified without the users knowledge in order to induce errors.

9. Cyber terrorism is not only limited to paralyzing computer infrastructures but it has gone far beyond that. It is also the use of computers, Internet and information gateways to support the traditional forms of terrorism like suicide bombings. Internet and email can be used for organizing a terrorist attack also. Most common usage of Internet is by designing and uploading websites on which false propaganda can be pasted. This comes under the category of using technology for psychological warfare.

Tools of Cyber Terrorism

10. Cyber terrorists use certain tools and methods to unleash this new age terrorism. These are :-

- (a) **Hacking.** The most popular method used by a terrorist. It is a generic term used for any kind of unauthorized access to a computer or a network of computers. Some ingredient technologies like packet sniffing, tempest attack, password cracking and buffer overflow facilitates hacking.
- (b) **Trojans.** Programmes which pretend to do one thing while actually they are meant for doing something different, like the wooden Trojan Horse of the 12th Century BC.
- (c) **Computer Viruses.** It is a computer programme, which infects other computer, programmes by modifying them. They spread very fast.
- (d) **Computer Worms.** The term 'worm' in relation to computers is a self contained programme or a set of programmes that is able to spread functional copies of itself or its segments to other computer systems usually via network connections.
- (e) **E-Mail Related Crime.** Usually worms and viruses have to attach themselves to a host programme to be injected. Certain emails are used as host by viruses and worms. E-mails are also used for spreading disinformation, threats and defamatory stuff.
- (f) **Denial of Service** These attacks are aimed at denying authorized persons access to a computer or computer network.
- (g) **Cryptology.** Terrorists have started using encryption, high frequency encrypted voice/data links etc. It would be a Herculean task to decrypt the information terrorist is sending by using a 512 bit symmetric encryption.

Challenges to India's National Security

11. As brought out earlier India has carried a niche for itself in the IT Sector. India's reliance on technology also reflects from the fact that India is shifting gears by entering into facets of e-governance. India has already brought sectors like income tax, passports, visa under the realm of e-governance. Sectors like police and judiciary are to follow. The travel sector is also heavily reliant on this. Most of the Indian banks have gone on full-scale computerization. This has also brought in concepts of e-commerce and e-banking. The stock markets have also not remained immune. To create havoc in the country these are lucrative targets to paralyze the economic and financial institutions. The damage done can be catastrophic and irreversible.

Existing Counter Cyber Security Initiatives.

12. **National Informatics Centre (NIC).** A premier organisation providing network backbone and e-governance support to the Central Government, State Governments, Union Territories, Districts and other Governments bodies. It provides wide range of information and communication technology services including nation wide communication

Network for decentralized planning improvement in Government services and wider transparency of national and local governments.

13. Indian Computer Emergency Response Team (Cert-In). Cert-In is the most important constituent of India's cyber community. Its mandate states, 'ensure security of cyber space in the country by enhancing the security communications and information infrastructure, through proactive action and effective collaboration aimed at security incident prevention and response and security assurance'.

14. National Information Security Assurance Programme (NISAP). This is for Government and critical infrastructures, Highlights are :-

- (a) Government and critical infrastructures should have a security policy and create a point of contact.
- (b) Mandatory for organizations to implement security control and report any security incident to Cert-In.
- (c) Cert-In to create a panel of auditor for IT security.
- (d) All organizations to be subject to a third party audit from this panel once a year.
- (e) Cert-In to be reported about security compliance on periodic basis by the organizations.

15. Indo-US Cyber Security Forum (IUSCSF). Under this forum (set up in 2001) high power delegations from both side met and several initiatives were announced. Highlights are :-

- (a) Setting up an India Information Sharing and Analysis Centre (ISAC) for better cooperation in anti hacking measures.
- (b) Setting up India Anti Bot Alliance to raise awareness about the emerging threats in cyberspace by the Confederation of Indian Industry (CII).
- (c) Ongoing cooperation between India's Standardization Testing and Quality Certification (STQC) and the US National Institute of Standards and Technology (NIST) would be expanded to new areas.
- (d) The R&D group will work on the hard problems of cyber security. Cyber forensics and anti spasm research.
- (e) Chalked the way for intensifying bilateral cooperation to control cyber crime between the two countries.

Challenges and Concerns.

16. Some challenges and concerns are highlighted below :-
- (a) Lack of awareness and the culture of cyber security at individual as well as institutional level.
 - (b) Lack of trained and qualified manpower to implement the counter measures.
 - (c) Too many information security organisations which have become weak due to 'turf wars' or financial compulsions.
 - (d) A weak IT Act which has become redundant due to non exploitation and age old cyber laws.
 - (e) No e-mail account policy especially for the defence forces, police and the agency personnel.
 - (f) Cyber attacks have come not only from terrorists but also from neighboring countries inimical to our National interests.

Recommendations.

17. 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.

Conclusions.

18. 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.