CYBER TERRORISM: WORLD WIDE WEAPONISATION!

Shubham Chaudhary[1]

Abstract

It is more than obvious that the way of conducting terrorism with the time is becoming more sophisticated. The cyberterrorism is real threat to fast technology development. Potential targets are systems which control the nation's defences and critical infrastructure. The terrorist of the future will win the wars without firing a shot - just by destroying infrastructure that significantly relies on information technology. The fast growth of the Internet users and Internet dependance dramatically increased the security risks, unless there are appropriate security measures to help prevention. To understand cyber terrorism it is important to look at its background, to see how the terrorist organisations or individuals are using the advantage of new technology and what kind of measures governments are taking to help the fight against cyber terrorism.This paper tries to gives a descriptive and analytical picture of cyber terrorism in India.The paperenvisages 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. Finally, the paper discusses some of the major incidents of cyber terrorism that have ravaged the real and virtual worlds in the recent past.

Keywords: Technology, Cyber world, Terrorism, Internet,

Introduction

A new page in the Information warfare book comes in a sinister form. Cyber-terrorism involves highly targeted efforts made with the intention of terrorism. It is an emerging threat that has the potential to cause serious damage. While we'd often associate terrorism with loss of life, we cannot overlook important results like intimidation or coercion that can be brought about by cyber-terrorism. Cyber space is regarded as the meeting place for criminal groups.[2]Cyber space has recently emerged as the latest battleground in this digital age.[3] The convergence of the physical and virtual worlds has resulted in the creation of a "new threat" called Cyber terrorism.

[1]3rdYear, B.A. LLB. (Hons.) Dr. Ram ManoharLohiya National Law University, Lucknow
[2]Tushabe and Baryamureeba 2005 World Academy of Science, Engineering and Technology
[3]Veerasamy 2009 4th International Conference on Information Warfare and Security 26-27 March

The word "Cyber Terrorism" is of recent vintage and was coined by computer whiz Barry C. Collin. The term cyber terrorism has been attempted to be defined from various angles. According to the definition provided by the US national infrastructure protection centre (2001), cyber terrorism may mean a criminal act perpetrated by the use of computers and telecommunication capabilities resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty with a given population with the goal of influencing a government or population to conform to particular political, social or ideological agenda[4]. The term has also been defined by the International Handbook on Critical Information Infrastructure Protection[5], as "attacks or series of attacks on critical information carried out by terrorists and instils fear by effects that are disruptive or destructive and has a political , religious and ideological motivation"[6]. From the above literature, it could be understood that cyber terrorism is not a new phenomena. This is a criminal conduct in the cyber space to disrupt peaceful governance. Can all cyber crimes be called as cyber terrorism ? Not really. It is pertinent to note that while all cyber terrorism cases are cyber crimes, not all cyber crimes can be called acts of cyber terrorism. Only those cyber crimes which are politically or ideologically motivated qualify to be called as acts of cyber terrorism .In the year 2000, an engineer working in Maroochy Shire Waste Water Plant ,Sunshire Coast City, Australia subverted the computers of the company which controlled its operations , to vent out his feelings of frustration with the company's promotion policies. The result was release of millions of tons of sewage water into parks and seacoast of the city causing massive environmental damage. As the act was not ideologically or politically motivated , it was not, rightly so, called an act of cyber terrorism. It was a grave cyber crime, never the less.

The main aim of cyber terrorists today is to cripple critical infrastructure of a country by cyber attacks to further the causes they espouse for as a terrorist group. In their wish lists are critical infrastructure like telecommunications, electric grids, transportation networks, banking & finance, water supply , fuel production & supply chains, military complexes , government operations .and emergency services. Some researcher have established that cyber terrorism includes two main types of activities, viz., cyber crime and misuse of information technology, and therefore it would be wrong to assume that cyber terrorism is a new kind of cyber crime[7]. It

[4]Denning, D. E. (2010). Terror's Web: How the Internet is transforming Terrorism. In Y. Jewkes& M. Yar (Eds.), Handbook of Internet Crimes (pp. 194 - 213). Cullumpton: Willan Publishing

[5] (CIIP) 2006 Vol. II

[6]Schjolberg, S. (2007) Terrorism in Cyberspace - Myth or reality? Retrieved 12 August 2011 from http:// www.cybercrimelaw.net/documents/Cyberterrorism.pdf

[7]Schjolberg, S. (2007) Terrorism in Cyberspace - Myth or reality? Retrieved 12 August 2011 from http:// www.cybercrimelaw.net/documents/Cyberterrorism.pdf

may be worthy to note that the types of cyber crimes that are involved in cyber terrorism may vary from identity theft[8], to denial of service attack[9]. 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. Unlike the terrorists that place their camps in countries with weak governance, cyber terrorists can store anywhere and remain anonymous.[10]Even though countries like the US had developed and is still developing strategic methods to combat cyber terrorism, lack of focused law, proper infrastructure and trained experts to trace the details of the extremist pose serious problems for countries like India to combat terrorism in cyber space.

TOOLS OF TERROR

Cyber terrorists use various tools and methods to unleash their terrorism. Some of the major tools and methodologies are discussed below:

1. Hacking: "Hacking" is a generic term for all forms of unauthorised access to a computer or a computer network. Hacking can manifest itself in many ugly forms including "cyber murders". A British hacker hacked into a Liverpool hospital in 1994 and changed the medical prescriptions for the patients. A nine-year-old patient who was "prescribed" a highly toxic mixture survived only because a nurse decided to re-check his prescription. The hacker's motive – he wanted to know "what kind of chaos could be caused by penetrating the hospital computer" Others have not been so lucky. An underworld don who was only injured in a shoot out was killed by an overdose of penicillin after a hacker broke into the hospital computers and altered his prescription.Hacking is facilitated by many technologies, the major ones being packet sniffing[11], tempest attack[12], password cracking and buffer overflow[13]

[8]Wykes, M. &Harcus, D. (2010). Cyber-terror: construction, criminalisation and control. In Y. Jewkes& M. Yar (Eds.), Handbook of Internet Crimes (pp. 214 - 229). Cullumpton: Willan Publishing

[9] Denning, D. E. (2010). Terror's Web: How the Internet is transforming Terrorism. In Y. Jewkes& M. Yar (Eds.), Handbook of Internet Crimes (pp. 194 - 213). Cullumpton: Willan Publishing.

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

[11]When information is sent over computer networks, it gets converted into hex and broken into lots of packets. Each packet is identified by a header, which contains the source, destination, size of packet, total number of packets, serial number of that packet, etc. If a hacker wants to see this information, he uses Packet Sniffing technology that reconverts the data from hex to the original. This technology is like putting the equivalent of a phone tap on a computer. Sniffing can be committed when a packet leaves the source or just before it reaches the destination. For

2. Computer Viruses: A computer virus is a computer program that can infect other computer programs by modifying them in such a way as to include a copy of it. Viruses are very dangerous; they are spreading faster than they are being stopped, and even the least harmful of viruses could be fatal. For example, a virus that stops a hospital lifesupport computer could be fatal. Over the years thousands of viruses have ravaged the information of computer users, the most infamous ones being Melissa[14], ExploreZip, Chernoby, Pakistani Brain[15], Stoned-Marijuana[16], Cascade and Michelangelo[17].

3. Computer Worms: The term "worm", in relation to computers, was used for the first time by science fiction author John Brunner in his book called "The Shockwave Rider". A computer worm is a self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems (usually via network connections). Unlike viruses, worms do not need to attach themselves to a host program. There are two types of worms – host computer worms and network worms[18]. The first computer worm was developed for the assistance of air traffic controllers in 1971. This "worm" programme would notify air traffic controllers when the controls of a plane moved from one computer to another. In fact, this worm named "creeper" would travel from one computer screen to the other on the network showing the message, "I'm creeper! Catch me if you can!" The difference was that this creeper did not reproduce

this, the hacker would need to know only the IP Address (the unique number that identifies each computer on a network). A packet sniffer can log all the files coming from a computer. It can also be programmed to give only a certain type of information – e.g. only passwords.

[12] TEMPEST (Transient Electromagnetic Pulse Emanation Standard) technology allows someone not in the vicinity to capture the electromagnetic emissions from a computer and thus view whatever is on the monitor. A properly equipped car can park near the target area and pick up everything shown on the screen. There are some fonts that remove the high-frequency emissions, and thus severely reduce the ability to view the text on the screen from a remote location. This attack can be avoided by shielding computer equipment and cabling.

[13] Also known as buffer overrun, input overflow and unchecked buffer overflow, this is probably the simplest way of hacking a computer. It involves input of excessive data into a computer. The excess data "overflows" into other areas of the computer's memory. This allows the hacker to insert executable code along with the input, thus enabling the hacker to break into the computer.

[14] This virus, when it was first noticed on 26th March 1999 was the fastest spreading virus the world over. The virus by itself was quite harmless. It merely inserted some text into a document at a specified time of the day. What caused the maximum harm was that the virus would send itself to all the email addresses in the victim's address book. This generated enormous volume of traffic making servers all over the world crash.

[15] This is the first virus known to have spread all over the world.

[16] This virus was originally written in New Zealand and would regularly display a message, which said, "Your PC is stoned. Legalize Marijuana

[17] This virus is titled after famous Italian Renaissance artist Michelangelo Buonarroti. It gets activated every year on the artist's birthday – 6th March

[18] Network worms consist of multiple parts (called "segments"), each running on different machines (and possibly performing different actions), using the network for several communication purposes. Network worms that have one main segment, which coordinates the work of the other segments are sometimes called "octopuses

itself. The world has seen thousands of worms, the more (in)famous ones being the Internet Worm, the SPAN network worm[19] and the Christmas tree Worm.[20]

4. Email Related Crime : Email has emerged as the world's most preferred form of communication. Like any other form of communication, email is also misused by criminals. The ease, speed and relative anonymity of email has made it a powerful tool for criminals. Some of the major email related crimes are email spoofing, spreading Trojans, viruses and worms; email bombing[21], threatening emails, defamatory emails.

5. Denial of Service Attacks : In January 2002, Cloud Nine, a UK based Internet Service Provider (ISP), was forced to shut shop after a week-long Denial of Service attack (DoS) resulted in the complete stoppage of its service. Denial of Service (DoS) attacks are aimed at denying authorized persons access to a computer or computer network. These attacks may be launched using a single computer or millions of computers across the world. In the latter scenario, the attack is known as a distributed denial of service (DDoS) attack.
6. Cryptography A disturbing trend that is emerging nowadays is the increasing use of encryption, highfrequency encrypted voice/data links, steganography etc. by terrorists and members of organized crime cartels. Notable examples are those of Osama bin Laden[22], Ramsey Yousef[23], Leary[24], the Cali cartel[25], the Dutch underworld[26]and the Italian mafia

[19] On the 16th of October 1989, a worm named WANK infected many computers on a network. This worm, if it found that it had system privileges, would change the system announcement message to "Worms against Nuclear Killers!" The message was graphically shown as the first letters of each word and the last three letters of the last word

[20] The Christmas tree worm was a combination of a Trojan horse and a chain letter. This mainframe worm managed to paralyze the IBM network on Christmas day 1987. The worm was written in a language called Exec. It asked the user to type the word "Christmas" on the screen. Then it drew a Christmas tree and sent itself to all the names of people stored in the user files "Names" and "Netlog" and in this way propagating itself.

[21] Email bombing refers to sending a large number of emails to the victim causing his email server to crash.

[22]The alleged mastermind behind the September 11 attack on the World Trade Center in the USA is believed to use steganography and 512-bit encryption to keep his communication channels secure

[23] He was behind the bombing the World Trade Center in the USA in 1993 and an aircraft belonging to Manila Air in 1995.

[24] He was sentenced to 94 years in prison for setting off fire bombs in the New York (USA) subway system in 1995. Leary had developed his own algorithm for encrypting the files on his computer.

[25] This cartel is reputed to be using sophisticated encryption to conceal their telephone communications, radios that distort voices, video phones which provide visual authentication of the caller's identity, and instruments for scrambling transmissions from computer modems.

Different uses of the Internet by Terrorist groups:

The long-held belief that terrorists are unorganized and non-technical has been clearly shattered in modern times. Organised crime and terrorist groups are using sophisticated computer technology to bypass government detection and carry out destructive acts of violence.It has been reported that the first known attack by terrorists against a country's computer system took place in Sri Lanka in 1998, when the ethnic Tamil Tigers guerrillas overwhelmed Sri Lankan embassies with 800 e-mails a day over a two week period.[27] These messages threatened massive disruption of communications and caused fear and panic among ordinary Sri Lankans as the rebel group was notorious for killing people. During the war in Kosovo in 1999, Serb sympathisers tried to target the NATO website with viruses.[28] Internet saboteurs in 1998 attacked Web site of the Indian Bhabha Atomic Research Centre and stole e-mails from the same center. The three anonymous saboteurs through online interview claimed that they protest against recent nuclear explosions in India[29]

In October 2007, hackers attacked the Web site of Ukrainian President Viktor Jush-enko. The responsibility for this attack took over the radical Russian nationalist youth group, the Eurasian Youth Movement[30]. In another incident, cyber attacks were launched against the Estonian state during April 2007. The targets were the Estonian Parliament, banks, media houses and government departments. These attacks affected critical services. The events in Estonia illustrated how countries can be put at risk by attacks via the Internet.[31].

---

[26] Dutch organized crime syndicates use PGP and PGPfone to encrypt their communications. They also use palmtop computers installed with Secure Device, a Dutch software product for encrypting data with IDEA. The palmtops serve as an unmarked police / intelligence vehicles database.

[27] See Tushabe&Baryamureeba (n 1) 67; Also see Denning (n 9) 7. Also see Walker 2006 "Cyber –Terrorism: United Kingdom" 635

[28] Walker (n 30) 635. Chinese computer hackers also launched attacks on US web sites to protest against NATO's bombing of a Chinese embassy in Kosovo. See Krapp (n 13) 72

[29]Wireless network hacks and mods for dummies, 2005, Wiley

[30] Radio Free Europe, 2007

[31] See Veerasamy "Conceptual Framework" 4. Also see Brunst (n 12) 62

An analyst from the U.S. Central Intelligence Agency (CIA) publicly revealed that in January 2008, hackers successfully stopped power supply networks in several U.S. cities. In November 2008, the Pentagon had a problem with cyber attacks carried out by computer virus, prompting the Department of Defense (DoD) to take unprec-edented step of banning the use of external hardware devices, such as flash memory devices and DVDs.,[32] Officially U.S. never felt cyber terrorist attack.

On the other hand, terrorists can also use the Internet for organisational purposes rather than to commit acts of terror. Terrorists can use the computer to commit various crimes such as identity theft, computer viruses, hacking, malware, destruction or manipulation of data. Terrorists can use information communication technologies (ICTs) and the Internet for different purposes: propaganda, information gathering, preparation of real-world attacks, publication of training material, communication, terrorist financing and attacks against critical infrastructures.[33] This means that organisations or governments which depend on the operation of computers and computer networks can be easily attacked. The Internet has the advantage of being "a more immediate, individual, dynamic, in-depth, interactive anonymous, unedited, cheaper and far-reaching process than conventional media". These factors facilitate the task of terrorists to execute their plans unhindered.[34]

Indian Interpretation of Cyber Terrorism

Even though the issue of cyber terrorism has attracted huge attention from cyber criminologists, cyber law specialists and social science researchers, very few researches have been done for analyzing the legal issues involved in cyber terrorism in India.

A minute analysis of the 26/11 Mumbai attacks would show that cyber communication between the terrorists and usage of cyber technology by them to be acquainted with the target population and the place, created similar devastating results in India. It was observed that most of the 26/11 planning was also planned meticulously with Google Earth. The terrorists made use of "cellular phone networks for command and control, as well as social media to track and thwart the efforts of Indian commandos.More worryingly, the terrorists demonstrated expertise which bore hallmarks of a professional team. They managed to convert audio signals to data before

[32] FOX News, 2008

[33]Gerke (n 34) 52-57. Also see Brunst (n 12) 70-73; 74-75; Walker (n 30) 635-642 and Conway (n 18) 4-10

[34]Raghavan (n 7) 297. It should be stated that the general motivations to commit crimes via the Internet are: the lack of a definite physical location, the use of bandwidth and speed of third parties to perpetrate cyber crimes, the anonymity of cyberspace, the lack of physical borders or boundaries and the cost- benefit ratio. For detailed discussion about these issues, see Brunst (n 12) 53-56

transmission. This made it almost impossible to Indian security forces detect and intercept given their current level of infrastructure and capabilities[35]

In July 2011, the digital technology was further used for bomb blasts in a crowded city market in Jhaveri Bazaar, Mumbai. The 2010 Varanasi blast case also saw the usage of cyber communication wherein the Indian Mujahiddin claimed responsibility for the blast.

Awakened by this, the Government of India took strong steps to strengthen the cyber security, including prohibition of terrorist activities through cyber space by way of amending the existing Indian information Technology Act, 2000. India was the 12th nation in the world to legislate on cyber law, adopting an IT Act, although the term "cyber terrorism" is absent from the terminology of the Act, as IT Act 2000 was first implemented by the Indian government to mainly "provide legal infrastructure for electronic commerce in India, and to facilitate electronic filing of documents with Government agencies" However, due to criticisms of the lack of legislations in ITA, Information Technology Amendment Act (ITAA) which contains a more holistic set of cybercrime laws such as inclusion of child pornography and cyber terrorism was then passed by the Parliament in 2008, Further GOI has also brought about amendments to the Indian Penal Code (IPC) and the Indian Evidence Act to aid in cyber crime investigation. The provision that was specifically inserted in this legislature for this purpose was section 66F which defines and describes cyber terrorism From the section 66F , it could be inferred that, cyber terrorism is an act of hacking, blocking and /or computer contaminating in order to restrict legally authorized persons to access computer resources in general, and /or to gain or obtain unauthorized access to any information which is a 'restricted information' for the purpose of security of the state, or foreign relation etc. These are gruesome acts which is done with an intention to threaten the security, sovereignty and integrity of India or strike terror in the minds of people or a section of people; and which may result in death and injury to people, damage to properties, disruption of civil services which are essential to the life of a community, and also affects the critical information infrastructure. For elaborating these characteristics, I take up the 26/11 Mumbai terror attack case. Even though the media had highlighted the phenomenal terrorist attack on crucial business and Jewish settlements in Mumbai, the Indian Ministry of Home affairs in their annual report (2010) had released a detailed nexus between digital technology and the misuse of the same by extremists, satellite phones, GPS and various websites

[35]Cyber Terrorism: The Fifth Domain. Retrieved October 10, 2012, from http://www.indiablooms.com/MedleyDetailsPage/medleyDetails040612a.php

were widely used for fulfilling the mission of the extremists.[36] As per the facts available regarding 26/11 attacks, the perpetrators did access the computer resources available at Taj Hotel and Trident Hotel. They accessed the Hotel computers to download information about the hotel guests, especially the US and UK citizens staying at that point of time. Their objective was to kill the hotel guest selectively by obtaining their room numbers from hotels computer database. What perpetrator did? From section 66F perspective, the perpetrators intentionally threatened the unity, integrity, security, or sovereignty of India and struck terror and caused death or injuries to the person and damaged or destruction of property by penetrating or accessing a computer resources without authorisation. Thus the act of perpetrator of 26/11 may fall under the category of cyber terrorism.[37]

The Information Technology Act, 2000 (amended in 2008) had painstakingly taken efforts to secure protected systems, which is defined by Section 70. "The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system". Further actions of government include the passing of rules such as the Information Technology (Guidelines for Cyber Cafe) Rules, 2011 under the umbrella of the IT Act. In doing so, the government has had to walk a fine balance between the fundamental rights to privacy under the Indian Constitution and national security requirements. Cyber terrorism gains new faces in pace with the growing innovations in the cyber field. India faces diverse challenges of cyber terrorism with the emergence and widespread use of social networking sites and digital medium. Significantly more than 80 internet pages were banned by the government of India in the wake of rumours after the Assam incident reveals the intensity of new face of cyber terrorism in the country.[38]

Existing Counter Cyber Security

Preparing against the threat of cyber-terrorism requires the same level of planning and preparation to survive an economic or financial crisis. One of the biggest concerns that

[36] Oh, O., Agrawal, M., & Rao, H. R. (2011) Information control and terrorism: Tracking the Mumbai terrorist attack through

[37] Pg-242, Vakul Sharma- Information technology

[38] Press trust of India (2012, Aug

organizations have when protecting against an emerging threat is the cost associated with it..The following initiatives[39] have been taken

A. National Informatics Centre (NIC): A premier organization 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 nationwide communication Network for decentralized planning improvement in Government services and wider transparency of national and local governments.

B. 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

C. National Information Security Assurance Program (NISAP): This is for Government and critical infrastructures, Highlights are Government and critical infrastructures should have a security policy and create a point of contact. Mandatory for organizations to implement security control and report any security incident to Cert-In. Cert-In to create a panel of auditor for IT security. All organizations to be subject to a third party audit from this panel once a year. Cert-In to be reported about security compliance on periodic basis by the organizations.

D. National Information Infrastructure Protection Centre (NIIPC): NIIPC is a designated agency to protect the critical information infrastructure in the country. It gathers intelligence and keeps a watch on emerging and imminent cyber threats in strategic sectors including National Defence. They would prepare threat assessment reports and facilitate sharing of such information and analysis among members of the Intelligence, Defence and Law enforcement agencies with a view to protecting these agencies' ability to collect, analyze and disseminate intelligence. NIIPC would interact with other incident response organizations including CERT-In, enabling such organizations to leverage the Intelligence agencies' analytical capabilities for providing advanced information of potential threats

.

[39] ids.nic.in, "Cyber Security in India's Counter Terrorism Strategy", Col SS Raghav

E. National Information Board (NIB): National Information Board is an apex agency with representatives from relevant Departments and agencies that form part of the critical minimum information infrastructure in the country. NIB is entrusted with the responsibility of enunciating the national policy on information security and coordination on all aspects of information security governance in the country. NIB is headed by the National Security Advisor.

F. 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.

These measures taken by the government to fight cyber terrorism must have the required coordination of Indian armed forces with cyber security agencies for crisis management action plan". The purpose is to facilitate and strategize better responses in times of crisis. The tight coordination of internal army forces with national organizations can be a a strategic plan by the government to counter cyber terrorism[40]

G. Department of Information Technology (DIT) : Department of Information Technology (DIT) is under the Ministry of Communications and Information Technology, Government of India. DIT strives to make India a global leading player in Information Technology and at the same time take the benefits of Information Technology to every walk of life for developing an empowered and inclusive society. It is mandated with the task of dealing with all issues related to promotion & policies in electronics & IT.

H. Standardisation, Testing and Quality Certification (STQC) Directorate STQC is a part of Department of Information Technology and is an internationally recognized Assurance Service providing organization. STQC has established nation-wide infrastructure and developed competentance to provide quality assurance and conformity assessment services in IT. Sector including Information Security and Software Testing/Certification. It has also established a

[40]PTI News Agency. (2010). Indian minister urges armed forces to prepare plan against cyber terrorism. BBC Monitoring South Asia - Political. Retrieved October 3, 2012, from www.lexisnexis.com/hottopics/lnacademic

test/evaluation facility for comprehensive testing of IT security products as per ISO 15408 common criteria security testing standards.

Conclusion

The exponential growth of cyberspace is possibly the greatest development of the current century .Information technology, the key to world success is blessed with many respects and several fall outs. The cyber crimes are the dark side of information revolution. In the current scenario, world is confronting with varied of terrorist threats where, cyber terrorism is a key one. The peculiar nature of cyberspace implies that existing laws are largely ineffective in curbing cyber crime and cyber terrorism, thus creating an urgent need to either modify existing legislation or to enact laws that are effective in checking the growing menace online. Apparently a legislation made to safeguard the e-commerce, cannot be pulled in to protect non-commercial issues including extremist communications and ideologies that are hatched in the cyber space. A minute analysis of the Information Technology Act, 2008 would show that the language of the provisions, especially section 69 F, fails to recognize the inherent meaning of terrorism through cyber space. Nothing but a focused law could be the answer for preventing cyber terrorist activities in India A law meant for safeguarding electronic commerce could go to save the personal data of the individuals, but it may not successfully envelop the issues of terrorism, even though such terrorist move could disrupt the commercial transactions through cyber space and thereby cause financial loss to the nation. It is submitted that this problem can be addressed not only though enacting stringent legislation and enhancing cyber security measures but also through international cooperation.Internet security is a global problem and cyber crime and cyberterrorism are increasingly becoming a worldwide nuisance.Cyberspace being the fifth common space, it is imperative that there be coordination, cooperation and uniformity of legal measures among all nations with respect to cyberspace.International cooperation will enable the nations of the world to crack downmore efficiently on cyber crime and ensure healthy development of the Internet. Countries must work together to introduce a set of core consensus crimes that can be enforceable against cyber criminals in any jurisdiction. Attempts that have been made so far, including the European Convention on Cyber crime or the OECD Guidelines and even the probable extension of LOAC to cyberspace are not without their respective glaring loopholes and deficiencies.Although the global fight against cyber terrorism is necessary, combating cyber terrorism should not jeopardise basic human rights and fundamental freedoms. To this end, “the urge to restrict, prohibit and to curtail must be resisted”. Therefore, countries

need to ensure that a balance is maintained between the protection of human rights and the need for effective prosecution.With state and judiciary acting hand in hand, citizens must also be encouraged to participate actively to weed out cyber terrorism. India must also look beyond its borders and foster cooperation with its partners. Cyber terrorism often presents a unique set of problems between two countries. As mentioned above, the country wherewith the terrorist is based on may decide it is better to keep at distance and not cooperate. Extradition of cyber terrorists is also difficult because the act in itself may seem too harmless for an extradition. The state must be kept lean and highly adaptive to enable a dynamic response to
Technologically innovative cyber terrorists. Technology is not static. It is an element that is
Constantly being updated and improved. Likewise, the state has to acclimatize quickly to these changes in technology and update itself constantly. This will prevent reliance on backdated solutions allowing India to effectively combat the latest cyber terrorist threats.

Recommendations

A. Security Policy and Assurance

1) Critical sector can be protected by improvising the software development techniques and system engineering practices. In order to secure critical sectors more strengthened security models should be adopted.

2) Better training must be provided in order to assist users in IT security.

B. Early Detection and response

1) To avoid malicious cyberspace activities rapid identification and information exchange methods should be adopted.

2) Identification of key areas within the critical infrastructure. 3) Establish a public – private architecture for responding to national- level cyber incidents.

C. Security training and Programs

1) National awareness programs such as National Information Security Assurance Program (NISAP) need to be promoted.

2) Providing training and education programs to support the Nation's cyber security needs

3) Increasing the efficiency of existing cyber security programs and improving domain specific training programs (such as: Law Enforcement, Judiciary, and E – Governance etc).

D. Promotions and Publicity 1) In India we need to organize various workshop programs, conferences, and research programs in various IT institutes to enhance cyber security skills. 2) The promotion and publicity campaign could include seminars, exhibitions, contests, radio and TV programs, videos on specific topics, Web casts, Leaflets and posters, suggestion and award schemes.

E. Specific Recommendations[41]:- 1) Emphasis should be placed on developing and implementing standards and best practices in government functioning as well as in the private sector. Cyber security audits should be made compulsory for networked organizations. The standards should be enforced through a combination of regulation and incentives to industry.

2) The government should launch a National Mission in Cyber Forensics to facilitate prosecution of cyber criminals and cyber terrorists.

3) The impact of the emergence of new social networking media, and convergence of technologies on society including business, economy, national security should be studied with the help of relevant experts, including political scientists, sociologists, anthropologists, psychologists, and law enforcement experts. It should be ensured that the issues of privacy and human rights are not lost sight of and a proper balance between national security imperatives and human rights and privacy is maintained.

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.

[41]Institute for Defense Studies and Analyses, India's cyber security Challenge, First Edition, March 2012

(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