Volume : 1 | Issue : 5 | Nov 2012 • ISSN No 2277 - 8160

Research Paper | Political Science

Varying Faces of Cyber Terrorism in India

S. Sreejith

Research Scholar (BPR&D Fellow), Dept. of Political Science & Public Administration, Annamalai University, Annamalai Nagar – 608 002, Tamil Nadu, India

ABSTRACT

Today terrorism and cybernetics have became highly allied terms where, the cybernetics intense the act of terrorism in to highly sophisticated and devastative one. Cyber warfare is the latest contribution of the twenty first century. Nowadays, the cyber net were highly used as the crucial tool in the terrorist arsenal to foster their activities. Irrespective of the common use of internet for the terrorist activities, terrorist groups in India uses new mode of action as social networks to gain maximum effect. The recent incidents of massive use of social networks for terrorist activities in India reveal the varying face of cyber terrorism and new challenges in the country.

KEYWORDS: Cyber terrorism, cybernetics, cyber warfare

Introduction

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 new face of terrorism uses cyber as means for terrorism purposes. It became the fertile platform for the terrorist to carry out their transnational activities. The internet for terrorist activities generates massive advantage for the terrorist groups through cyber attacks and poses greater challenge for the entire world communities.

Cyber terrorism is the vicarious form of cyber crime, severely threatens the security of the nation. Dorothy Denning defines "cyber terrorism as the convergence of terrorism and cyber space. It is understood to mean unlawful attack and threats of attack against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in the furtherance of political or social objectives"1. Mark Pollit also defines it as a "premeditated, politically motivated attack against information, computer systems, computer programmes and data which result in violence against non-combatant targets by sub national groups or clandestine agents"2.

Cyber terrorism is a greater challenge for India's national security where, several security establishments, business firms and national assets become vulnerable targets. As the cyber criminals, cyber field is potentially exploited by the terrorist to carry out their operations. The sensitive information essential for either government or security field are tracked by clandestine groups and misused by them. The stealing, disclosing or destroying of the vital information of national importance endangered the security of the nation. This is not only threatening the government or multinational companies but also harmful to the common civilian as the same. Internet and cyberspace also provide free medium of information transmission. The misuse of the medium for anti-national activities tarnishes the image of the nation and creates panic among the nationalities. At the same time, India, the growing giant in the IT field is severely challenged by the menace to drop out its position and development of the country. The last two decades of cyber operations by the non-combatant cyber terror groups continuing to emerge themselves as a greater threat to security of the nation.

Cyber Crimes and Cyber Terrorism

Cyber crimes are the offshoot of technological development where minor and major crimes from data theft to cyber terrorism were became common. The cyber medium became the cheap and easiest means to operate and produce critical impact. Dewang Mehta, President of India's National association of software companies (NASSCOM) stated cyber crimes is the crime of the future and it is now much more easily committed and less easily identified3. The terrorist opted critical national infrastructure as their soft targets through the same easiest way and produce desired impact.

India is one among the prime victim of cyber crime. The report of the Security and Defence Agenda (SDA), a leading defence and security think tank in Brussels and McAfee ranked India as the fifth country in the world severely harmed by cyber crimes4. The rose of cyber crimes from 2010 to 2011, 966 to 1791 cyber crime cases and 288 to 1184 arrests under IT act and 356 to 422 cases and 394 to 446 arrests under IPC act reported by National crime record bureau evident the far reaching growth of cyber crimes in India5. The then Home Minister of India stated cyber space as fifth domain after land, sea, air and space where much of country's critical infrastructure lies and challenged with terrorist threats6.

Cyber terrorism acclaimed its fame in India through several cyber activities as cyber attacks and terrorist facilities. As stated by Centre for strategic and international studies, it is "the use of computer network tools to shut down critical national infrastructures or to coerce or intimidate a government or civilian population"7. The cyber attacks in the forms of viruses and other means to disrupt the system, hacking and theft of data and denial of services by damaging networks etc., create harm especially in the government as well as essential service sectors.

Several government and security establishment sites in the country were incessantly targeted by such attacks. The IT Minister on November 30, 2011 in Lok sabha stated that 90, 119, 252, and 219 government web sites has been defaced by various hacker groups in the year 2008, 2009, 2010 and January- October 20118. The another statement by the minister reported, 112 government websites includes BSNL, Ministry of Finance, Planning commission and several state government agencies were hacked in three months just before march 20129. The large scale spreading of Trojan viruses also harmed the systems in the country.

The terrorist had also uses the cyber field for facilitating their activities as communication, banking, financial fraud etc. The investigation of David Hardly in US revealed that the hardly team used Mail service for communicating each other by saving messages in the draft and members visited the mail by using same passwords without sending each other. Terrorist in several attacks in India such as Ahmedabad (2008), Jaipur (2008), Delhi (2005) Varanasi (2010) and Delhi High court (2011) etc., have used the internet and mail services to further their attacks in Indian soil. Mumbai 26/11 operation reveals the extensive use of internet, mobile and satellite phones to communicate the directions from the planners and perpetrators in different spots.

Terrorist groups also use the web bases to recruit, train and motivate the followers for the jihadi move. Al Qaida, Laksher e Taiba, Indian Mujahedeen etc., are having their own IT wings which carry terrorist activities in the cyber field. The extensive arrests of IT professionals in terrorism related activities in the country in the immediate past give more weight for the claim of cyber terrorism in the country. Ronald Nobel, former Head of United States Secret Service who is the secretary general of the Interpol says in an interview that the internet is giving terrorists new ways to plot mass murders10.

Recent trends in India

Terrorist uses cyber means as a psychological weapon is common today. Irrespective of the traditional means of military or direct confrontation, the terrorist groups using internet to fight in psychological way. This cyber alternative helps them to produces immense effect with least cost of time and effort. The growing popularity of social networking facilitates terrorist to do it more easily. Terrorist groups shifted their plat form by using social networks to wide spread harm and distress among the communities.

Recent Assam incident in India is a classic example for the use of cyber means to hasten the issue and threatens the integrity in the country. The terror group misused the incident by spreading of morphed photographs and video clips through social networking sites such as Twitter and Facebook, MMS and mobile text messages to create social unrest among the communities. The Home Ministry report noted that email, chat rooms, VOIP calls and social media such as Face book, Twitter and You tube, were rampantly used to spread rumours by creating fake accounts in these sites11. It brought the local communal issue in to national hemisphere with international ramification. The investigation revealed the role of Pak based terrorists groups to sensationalise the issue of local communal violence in Assam in to country wide aggression by spreading rumours and fake news through internet. It led mass exodus of people belonging to North east from major Indian cities following the rumours of possible attack on them.

The widespread use of social networks by the terrorist groups to arose the religious and regional consciousness among the society and took maximum advantage from such activities. This created insecurity and large scale hatred among the communities which negatively affected the country's effort in integration. The Pak based hackers uses Indian accounts on social media cites and websites to spread panic across the country. They used these means for transcending fundamentalism and jihadi objectives to strengthen the fundamental elements among the civilian which detriments the national goal of secularism and fraternity. This psychological warfare further fuels the local issues and creates antinational mood which helps the terrorist to enjoy mass support for their cause.

Cyber Terrorism in India and Pakistani Link

As similar to the transportation of trans-border terrorist activities, Pakistan highly engaged to intensify cyber terrorism in India. The Pak based hackers and websites were used to propagate anti-India propaganda and instruction for cyber attacks in the country. The news report in Hindustan times reported in December 19, 2000 disclose that a number of Pakistani hacker groups as 'Death to India', 'Kill India' and 'G- Force of Pakistan' have openly circulated instruction for attacking Indian computers12. The cyber attack on CBI web site by 'Pakistan Cyber Army' in December 3, 201013 and BSNL web site by 'H4tr!ck' on December 4, 2012 were the recent attacks on countries top web sites by Pak hacker groups14.

The misuse of cyber space by Pakistani terrorist groups against India is clearly evident from the Mumbai 26/11 attack where, the planners established control room in Pakistan to direct the attack with the sophisticated cyber support. The tracking of rumours and false news about the recent Assam incident clearly exposed the Pakistani hand to create the internal disturbances in India. This reveals the Pak plot to attack the nation in cyber way.

Conclusion

Today the world is closely connected with the communication and information technology. These information and communication facilities are being misused by the terrorist groups for transcending their transnational activities and create greater thread to security of the nation. 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 country15. The growing cyber challenges in the country and its active role of Pakistan needs more national attention on the cyber space in the country to prevent further hazards.

REFERENCES

1. Michael Chance (2012), The role of cyber terrorism in the future, forensic focus, Retrieved from: http://articles.forensicfocus.com/2012/06/01/the-role-of-cyber-terrorism-in-the-future/, Accessed on: 12/09/2012. | 2. Medha Surabhi (2012), Cyber warfare and cyber terrorism, Social science research net, Retrieved from: http://ssrn.com/abstract=2122633, Accessed on: 15.09.2012. | 3. Press Trust of India (2012), Indian websites are new targets of Hawkers, Indian express, Retrieved on: http://www.cyberlawsindia.net/cases2.html, Accessed in: 12/05/2012. | 4. Sanchitha Bhattacharya (2012), Cyber terrorism: the fifth domain, South Asian Intelligence Review, Vol. 10 (48), Retrieved from: http://www.satp.org/satporgtp/sair/ Archives/sair10/10_48.htm, Accessed on: 14/09/2012. | 5. National crime record bureau (2011), The Crime- 2011 statistics, New Delhi. Retrieved from: http://ncrb.nic.in/CD-CII2011/cii-2011/Chapter%2018.pdf, Accessed on: 12/09/2012. | 6. Opcit., Sanchitha Bhattacharya (2012). | 7. James Lewis (2010), "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," Center for Strategic and International Studies, Retrieved from: http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf, Accessed on: 28/10/ 2010. | 8. Staff reporter (2012), 112 govt. Website hacked in three months, Economic times, Retrieved from: http://articles.economictimes.indiatimes.com/2012-03-15/news/31197171_1_ government-websites-internet-frauds-sachin-pilot, Accessed on: 10/09/2012. | 9. Opcit., Sanchitha Bhattacharya (2012). | 10. Vicky Nanjappa (2012, Jan. 10), Why India needs to tackle cyber terrorism, Retrieved from: http://www.rediff.com/news/report/why-india-needs-to-tackle-cyber-terrorism/20120101.htm, Accessed on: 15/08/2012. | 11. Staff reporter (2012, Aug. 19), Pakistani group morphed pictures to spread panic, says ministry report, Hindu business line, Retrieved from: http://www.thehindubusinessline.com/news/article3795413.ece, Accessed on: 25/09/12 | 12. Opcit., Sanchitha Bhattacharya (2012). | 13. Press trust of India (2010, Oct. 04), CBI website hacked by Pakistan cyber army, Hindustan times, Retrieved from: http://www.hindustantimes.com/News-Feed/SectorsInfotech/CBI-website-hacked-by-Pakistani-Cyber-Army/Article1-634141.aspx, Accessed on: 12/09/2012 | 14. Opcit., Economic times (2012). | 15. Press trust of India (2012, Aug. 19), Govt blocks 80 internet pages, user accounts, The Hindu, 12/08/2012, Retrieved from: | http://www.thehindu.com/news/national/article3795738.ece, Accessed on: 15/09/2012