Imperial Journal of Interdisciplinary Research (IJIR)
Vol-3, Issue-4, 2017
ISSN: 2454-1362, http://www.onlinejournal.in

Modern Terrorism and National Security in India

C. Arunkumar[1] & Dr. P. Sakthivel[2]
[1]Ph.D Research Scholar, Dept. of Political Science & Public Administration, Annamalai University
[2]Associate Professor, Dept. of Political Science & Public Administration, Annamalai University

***Abstract**: Modern terrorism slightly differs from conventional or traditional terrorism. that, in conventional or terrorism terrorists employed methods such as the sword, the poison elixir, hand-thrown bomb, pistol, and more recently the machine gun and plastic explosives to target government or civilians and very often it ended with heavy causalities. but as far as modern or neo terrorism is concerned, terrorist employed new tools and techniques such as internet, social medias, highly sophisticated technologies to wage cyber war against democratically elected government and its people. This paper examines the role of cyber technology such as ICT, internet, Malicious Software Programme, Mobile phones, social medias, etc., in the modern day terrorism as the terrorism becomes a serious threat to India's national security and integrity.*

***Key words:** Terrorism, technology, national security, Cyber crime, modern technology, hacking.*

Introduction

Since the partition of the country in 1947, India has been facing numerous issues such as poverty, unemployment, under employment, illiteracy, casteism, communalism, insurgency, terrorism and cross border terrorism, fundamentalism etc. Naturally these issues directly or indirectly threatened the existence of sovereignty, integrity and security of the nation. In the recent past, terrorism has emerged as a major threat to sovereignty, integrity and security of the nation and remains to be a stumbling block for the national development and security of its subjects.

Terrorism is considered as the systematic use or threatened to use violence to intimate a population or a Government inorder to achieve some political, religious or ideological goals. Terrorism can be defined as unease – inspiring methods of repeated violent action, employed by secret person, group or state and non-state actors, for characteristic, illegal or political reasons, whereby they targets physical identity and civilians of a country. In India, terrorism is considered as a threat to unity, peace, prosperity and communal harmony. It disfigures India's democratic institutions, culture and considered as a drain on India's human and material resources.

The advent of Information, Communication and Technology (ICT) had also significantly contributed for the penetration of terrorism not only in India but around the world also. Because of availability of most sophisticated and powerful technologies, terrorist need not opt for conventional weapons to target or subjudicate the government and common people. They often, in the recent past, used internet and other technological devices to execute their attack (or) cyber war against governments, people, institutions etc., These innovations have enabled terrorists to communicate with other radical outfits, as well as to gather intelligence and access information for planning, coordinating and executing attacks, for instance Pathankot and Uri sector attack.

Modern Terrorism

Modern terrorism slightly differs from conventional or traditional terrorism. that, in conventional or terrorism terrorists employed methods such as the sword, the poison elixir, hand-thrown bomb, pistol, and more recently the machine gun and plastic explosives to target government or civilians and very often it ended with heavy causalities. but as far as modern or neo terrorism is concerned, terrorist employed new tools and techniques such as internet, social medias, highly sophisticated technologies to wage cyber war against democratically elected government and its people. According to Global Terrorism Index (GTI), Terrorism has increased by 70 per cent in India from 2012 to 2013, with the number of deaths increasing from 238 to 404. The number of attacks also increased, with 55 more attacks in 2013 than 2012. However, the majority of terrorist attacks in India have low casualties. In 2013 around 70 per cent of attacks were non-lethal. There were attacks by 43 different terrorist groups who can be categorised into three groups such as Islamists, separatists and radical communists.

As per South Asian Terrorism Port, 191 civilians, 173 security personnel and 501 terrorists were killed in the year 2016. Jammu and Kashmir was tops in the list of fatalities with the death of 13 civilians, 84 security personnel and 163 terrorists.

Communist terrorist groups are by far the most frequent perpetrators and the main cause of deaths in India. Three Maoist communist groups claimed responsibility for 192 deaths in 2013, which was nearly half of all deaths from terrorism in India. Police are overwhelmingly the biggest targets of Maoists, accounting for half of all deaths and injuries. This is mainly through armed assaults, which killed 85, and bombings and explosions, which killed 43. Kidnapping is also a common tactic of the Maoists where it is often used as political tool to force the government to release Maoist prisoners. The majority of Maoist attacks occurred in the state of Bihar, Chhattisgarh and Jharkhand.

It is widely believed that, more than Maoist groups the Islamic terrorist groups such as Lashkar-e-Taiba (LeT) , Jaish-e-Mohammed (JeM), Students Islamic Movement of India (SIMI), Harkat-ul-Mujahideen, Indian Mujahideen etc. are responsible for instigating or indulged in terrorist activities in India. For instance, in 2013 three Islamist groups were responsible for around 15 per cent of deaths. Islamist groups in India commonly use armed assaults targeting the police or private citizens. In conventional terrorism, classic weapons such as hand-thrown bomb, pistol, and more recently the machine gun and plastic explosives etc., were used in order to destroy government buildings, important physical identity of the country and to kill innocent civilians. Whereas in modern world, terrorists are using most sophisticated technologies such as malicious software, electromagnetic and micro wave weapons, to destroy or target valuable and confidential government official data in cyberspace. The cyberspace is an environment without boundaries, a privileged place where terrorists find resources, make hate propaganda activities and from which it is possible to launch the attacks against enemies everywhere in the world.

As has been mentioned already, because of ICT these terrorist groups along with home-grown terrorists and its organisations systematically planned and execute cyber terrorism, often termed as modern terrorism, against India. They started to attack the most important, confidential official websites of union and state governments, stolen valuable information, destroyed online government data, spread powerful malware on the internet world etc.,

Technology and Terrorist Attacks

For example, Brazilian hackers targeted several Indian government websites and defaced their home pages in April, 2013. Most of these defaced websites have been pulled off the servers and the links have been throwing "site not found" messages. The hacker with the handle 'HighTech' replaced the homepages with a video which appeared to be shot with a 'vine' application. The video shows a man dressed as joker standing on roadside, while a vehicle through which the video is shot, cruises past him. It is not yet known, whether the entire data of the websites has been damaged or just the homepages vandalised. Of the 18 websites hacked, the defence website (*www.cdarndbblr.gov.in*) belonging to the Controller of Defence Accounts (R&D) in Bangalore was also targeted by the terrorist.

The official website of the Government of Kerala — www.kerala.gov.in — was also hacked on September 26, 2015 night by hackers suspected to be from Pakistan. The home page of the hacked website sported a picture of the national flag being burned and the messages *"Pakistan Zindabad"* and *"security is just an illusion."* The hacked homepage also carries what appears to be identity of the hacker; "hacked" by Faisal 1337", reads the hacked homepage, *"We are Team Pak Cyber Attacker"*. The Home Page also contains the website address www.Faisal1337.com.

Hacker groups from Indonesia and Pakistan have defaced websites (www.tnvkpmis.gov.in, www.tn.gov.in) of government of Tamil Nadu in the year 2016, raising concern over the cyber security in India. An Indian group 'Anon.India' defaced the website of Bihar State Development Corporation (www.bstdc.gov.in) to protest the blocking of some websites by the Bihar government. In November 2014, Pakistan-based hackers, who called themselves *'Pakistan Cyber Mafia Hackers'*, hacked two Gujarat government websites as well as three other websites. Out of the five websites hacked, two belonged to the Gujarat government, including the official website of Commissionerate of Higher Education (www.egyan.org.in) and the Agricultural Produce Market Committee of Ahmedabad (www.apmcahmedabad.com). Other websites, which they claimed to have hacked, include www.delhi-pharma.com, www.listtopcolleges.in and www.atnnetwork.in. They put up the list of the hacked websites on the wall of their Facebook page.

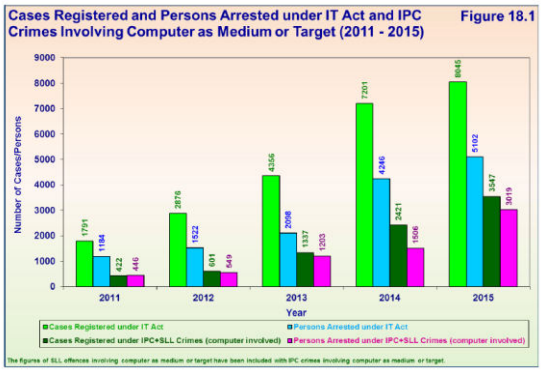
It is significant to note that, the Defence ministry official website was also hacked by terrorist groups and valuable data were also destroyed or stolen. Indian Computer Response Team (CERT-In) reported total number of 308,371 and 78 Government websites were hacked during the years 2011, 2012 and 2013. In a dramatic developments, the terrorists are using social YouTube, Viber, Snapchat, Wechat, Gab, Hike, Telegram, etc., to promote terrorism, showed the seeds of terrorism in the minds of young people in India. Further, the terrorists started to recruit people, especially the youths, for Jihadi

purposes through social medias inorder to carry out their hidden agendas in India. The arrest of terrorists in Hyderabad and Bangalore are ample evidence in this regard.

Indian Government had an excellent record of protecting its people, physical identity of the nation, nuclear assets etc., from terrorists attacks. Government has been taking numerous steps to improve the security of the nation. For example, on May 2005, the Indian Parliament had passed the Weapons of Mass Destruction and Their Delivery Systems (Prohibition of Unlawful Events) Bill, planned to avert the transfer of WMD, delivery systems, and associated technologies to state and non-state actors, including terrorists. The establishment of RAW (Research and Analysis Wing), IB (Intelligence Bureau), NIA (National Investigation Agency) and appointment of NSA (National Security Agency) considered as a milestone in combating terrorism. Significantly, these national level agencies in co-ordination with other state intelligence agencies such as anti-terrorism squads and cyber crime cell have combated several terrorist plots and attacks against civilians and achieved notable success in many terrorism related cases. At present our country is prepared to tackle the menace of modern terrorism or cyber terrorism through technology with the help of national security agencies.

Cyber Crime Under IT Act

In a report published by the National Crime Records Bureau report (NCRB 2015), 11,592 cases were registered under the cyber crimes (which includes cases under Information Technology Act, offences under related sections of IPC and offences under Special and Local Laws (SLL)) in comparison to 9,622 cases registered during the previous year (2014) which shows an increase of 20.5% over the previous year.



Uttar Pradesh has reported the highest number of such crimes accounting for 19.0% (2,208 cases out of 11,592 cases) of total cyber crimes followed by Maharashtra (2,195 cases out of 11,592 cases) accounting for 18.9% and Karnataka (1,447 cases out of 11,592 cases i.e. 12.5%). In these cases a total of 8,121 persons were arrested during 2015 in comparison to 5,752 persons arrested during the previous year (2014) registering 41.2% increase over the previous year. Uttar Pradesh (1,699) has reported the maximum number of persons arrested under such crimes.

Conclusion

The terrorist groups especially the LeT, JeM, SIMI, etc., are using the internet, social media and other platforms to recruit young Jihadist and brain washing the common people for executing their attack against the nation. It is significant to mention here, after the demonetisation announcement by the union government on 8th November, 2016 the instance of cyber fraud and crimes have increased to several folds. The RBI has setup a cyber security team but there seems to be not much decline in number of cybercrimes in India. When more and more number of online transaction will grow up and possibility of cyber fraud would also increase.

After China and USA, India was ranked third as a source of "malicious activity" on the internet and second as a source of "malicious code" cybercrimes. The NCRB data shows the nine time increase of cyber crimes from 569 in 2009 to 5752 in 2014. Despite the existing laws such as IT act, the IPC and other state and centre level legislations the number of cases registered under these acts have increased by more than 350 per cent from 2011 to 2015. Similarly number of persons arrested related with cybercrimes have also increased considerably. Maharastra tops in the list of cybercrimes for the period 2011 to 2015, Uttar Pradesh stands second and Karnataka with third place. The union government on several occasions issues advisories to state governments and union territories on cybercrimes but the trend is increasing every day. The government urged the states and union territories to build necessary technical capacity in handling cybercrime including technical infrastructure, cyber police stations and trained manpower for detection, registration investigation and prosecution of cybercrimes.

Indian Computer Emergency Response Team (CERT-In) and Centre for Development of Advanced Computing (CDAC), CBI, IB RAW etc., are significantly assisting both centre and state governments in fighting the menace of cyber terrorism.

The study found that, most important government websites, including the defence, finance, banking, ministries websites, NGT website etc., must be protected with the help of improved software development techniques and system engineering practices. Further, more improved and strengthened security models should be adopted in order the protect these websites from the hackers. National

awareness programmes such as National Information Security Assurance Programme (NISAP) intended to disseminate information about the evils of cybercrimes to government officials and general public, should be conducted periodically.

Routine and periodic 'Cyber Security Audit' should be conducted in order to review the strength and weakness of our cyber security systems, models, softwares so as to further improve the quality of functioning of these systems. The impact of social media networking in India on the National Security System should be studied comprehensively so as to understand the minds of the people especially with regard to social interaction between different radical outfits or groups. At present cybercrime cells are functioning only in district capitals and metropolitan cities only. But establishing such cells in other areas is very essential for controlling and eliminating such cybercrimes. More importantly, the prosecutors and cyber police must have enough resources, training and equipment's required to deal with the menace of modern terrorism.

Finally the centre and state governments must adopt integrated, comprehensive and more scientific approach to protect the government websites and other valuable information's from any kind of cyber threats or attacks. By adopting these measures alone can help the government to address the issue cybercrimes very effectively and can protect the national security and integrity of the country in a more effective manner.

References

[1] Ministry of Home Affairs. *"RGI releases Census 2011 data on Population by Religious Communities."* Press Information Bureau Government of India. 25-Aug.-2015. web. 12 Jan.2016.

[2] National Consortium for the Study of Terrorism and Responses to Terrorism. *"GTD Global Terrorism Database."* START (2015): 63. Web.

[3] Institute for Economics and Peace. *"Global Peace Index 2015: Quantifying Peace and Its Benefits."* Institute for Economics and Peace (2015): 120.

[4] Srinivas Reddy. *"Brazilian hacker defaces many Indian websites." The Hindu*. 6 April 2013. Hyderabad. web. 25 Aug. 2015.

[5] PTI. *"Government of Kerala Website Was Hacked by suspected Pakistani Hackers" – Tech2Firstpost*. 2015. Web. 28 Sep. 2016.

[6] Waqas. *"8 Indian Government Websites Hacked by Pakistani and Indonesian Hacker."* HackRead. N.p. 2015. Web. 12 Aug. 2016.

[7] PTI. "Pakistani Hackers Deface Two Gujarat Government Websites." *The Hindu*. 26 May. 2016. Ahmedabad. web. 27 May 2016.

[8] Computer era. "*IT minister Ravi Shankar Prasad revealed Cyber Crime statistics in India."* Computer Era & Sridhar Nallatmothu. 5 May 2016. Web. 24 July 2016.

[8] "Terrorism." *New World Encyclopedia*. 25 Nov 2015, 20:51 UTC. 16 Dec 2016.

[9] Franklin, Ursula M. *"The real world of technology."* House of Anansi, 1999.

[10] Warikoo, K. "Islamist Extremism: Challenge to Security in South Asia". Strategic Analysis,30.1(2006): 30-45.

[11] Bahadur, Kalim. "Regional Implications of the Rise of Islamic Fundamentalism in Pakistan". Strategic Analysis, 30.1(2006): 7-29.

[12] Prabha. Kshitij. "Defining Terrorism, Strategic Analysis". 24.1(2000).

[12] Krishna, Ashok. "Insurgency in the Contemporary World: Some Theoretical Aspects-Part II". Strategic Analysis, 21.9(1997).

[13] Saikia, Jaideep., and Ekaterina Stepanova, eds. Terrorism: Patterns of Internationalization. Sage Publications India Pvt. Ltd: New Delhi, 2009.