Studies in Indian Place Names
(UGC CARE Journal)
ISSN: 2394-3114
Vol-40-Issue-68-March-2020

Cyber Terrorism and India's National Security

Dr. P. A. Ghosh
Defence and Strategic Studies Department, Bhonsala Military College, Nashik

Manojit Das
Department of Political Science, Goa University, Goa

CHANGING CONCEPT OF SECURITY

The concept of national Security has been understood to denote protection of core values through the use of national power. It is, therefore, multidimensional, and includes military, political, economic and socio-cultural dimensions. The origins of the concept of national security may be found in the historical formulations of the concept of national interest. The expectations were that policy makers would rise above narrow and sectarian interest to focus on the issues that deal with the nation as a whole. National security thus "comprises every action by which a society seeks to assure its survival and realizes its aspiration internationally; the challenges we are facing are new. Also, all these are unpredictable and dynamic therefore we cannot conceptualize strategic perspectives ignoring the recent trends of the dynamics of the society. Because, the last two decades have brought into sharp focus an alarming and at times disastrous processes in the relationship between man and man and countries. Newly independent and developing countries where people's behaviour is passing through a transitional phase under different socio-political and eco-ethnic compulsion and thrust of modernizations continuously increasing with age old tradition, contains in itself different problems of the present time. New trends in security environment require wide-ranging review for clear understanding of people security problem worldwide. Comprehensive security is concerned with the problems of everyday life. It is not only concerned with weapons; rather it is concerned with the condition of human life and feelings in terms of individual safety and security; including armed forces personnel. [1]

The legitimate concern of the ordinary people is to ensure security in their daily lives. For many, security symbolizes protection from any kind of threats like diseases, crime, social conflict, political repression, environmental hazards, displacement etc. Hence, Security consists not only of military aspects, but also political, economic, social, human rights and ecological aspects. Under development and declining prospects for development, as well as mismanagement of resources, constitute challenges to security. The security of individuals and communities of which states are constituted is ensured by the guarantee and effective exercise of individual freedom, political, social and economic rights as well as by the preservation or restoration of inhabitable environment for present and future generations. Moreover, security also implies that essential human needs, in the field of nutrition, education, housing and public health are ensured on a permanent basis. A nation has security when its people don't have to compromise to their value of life and have feelings of security, and thus states do not have any threat of military aggression, political pressure or economic oppression etc. Thus, states are able to pursue freely their own developmental activities and progress. Thus, the imperative necessity is to have good governance to achieve the ends of both state and individual security. As an organizing concept of in international relations, the idea of national security provides us with several advantages. It helps us to focus on common elements and uniformities in external policies of nations are structured. Second, it helps us to focus on the underlying unity of internal and external activities of the state. It recognizes that external behaviour of states is an integral part of the total behaviour of the state and that the internal and external security is essentially interlinked. [2]

NATIONAL INTEREST

Defined within the context of the core values of a nation as identified by the constitution; defined as being a product of history (civilization) ; the value systems of the polity, economy and society and culture. The determining factors are the geography; the geo-political, economic and socio-cultural aspects that go into determine the core values.

Copyright © 2020 Authors

ISSN: 2394-3114
Vol-40-Issue-68-March-2020

NATIONAL POWER

National power refers to the capability of the nation-states to protect its national interests. Traditional definitions of national power have always projected military capability as the key element since traditional analysis of national interest had been confined to the narrow domain of national security. The interpretations of what constitutes national power have also undergone a change. The cold war era linkage of national security with military security underwent its first change during the seventies. The oil crisis and related developments brought in the interdependency approach to international relations. This was the time when discussions about economic components of power were being made and the linkage of national security with economic security was most prominent. In due course, in the post – cold war years, technology has come to dominate the debates on national power and with that the technological aspects have come to be highlighted. Protection of core values and therefore of national interest, is dependent upon the national power of the nation state (capability factor). National power is dependent upon the non-material elements that contribute to power.[3] **Security Strategy;** Strategy is the bridge that relates military power to political purpose; it is the use that made of forces and the threat of force for the ends of policy. War not only play role of merely political act but also a real political instrument; determine both aim of military force and also the amount of efforts to be made. Given the broader application of the concept of national security, strategy is not just about campaigns, but deals with peace time applications also. **Strategic culture;** the subcontinent is passing through a delicate period and peace and stability are still eluding. South Asia is emerging as a home to the component of modern instability. Proliferation of small arms and the nexus between Norco-terrorism and the expanding empires of non-state actor make this region volatile. India has its own share of disturbances in Jammu and Kashmir (J&K), heartland India (Left Wing Extremist) and the North Eastern region.

AIM OF THE PAPER

1. To address how information warfare and cyber terrorism pose challenges to individual, national and international security environment in the context of cyber crime; without the use of organized and structural violence. Cyber terrorism threat is real which requires immediate attention and action from citizens, law enforcement officials and public policy makers.

HYPOTHESIS

1 The senses of security in the mind of the people have been affected due to the increased dependency on internet and due to cyber crime.

METHODOLOGIES

1. The main aim of the present study is to have overall perspectives about national and international security with a special focus to cybercrime; current trends of events, facts, and attitudes. Against such background, the present work followed completely historical and analytical approaches and focuses to qualitative facts for which the induction and deduction methods are followed; based on observation and current events. Primary and secondary data have been collected and used from different magazines, internet, research journals, including government data.

CYBER TERRORISM: CONCEPT AND DIMENSION

Cyber terrorism in the era of information and communication technology is not limited to local and regional level has become catastrophic in nature and has succeeded in extending its global reach. This has been largely attributed to the computer and the internet with the success of new media. New media is a digital platform that provides access to digital information over the internet to web users through the medium of electronic devices and computer technology. This digital information technology includes websites, web pages, web applications, online radio, live broadcast, live webcast, live TV and social media handles, which include face book, twitter and instant messaging services like watts app and telegram. Old media is that platform, which provides information in the print medium. It includes printed newspaper, magazine, books, radio and any other such non – interactive media.

Terrorist and terrorist organisations that use computer technology as a weapon of the instrument in order to carry out terrorist activities over the internet, while gain publicity and attention given by new media gives rise to a new phenomenon that is cyber terrorism. Barry Collin, a senior research fellow at the Institute of security and intelligence, define cyber terrorism as the convergence of cybernetic and

Copyright © 2020 Authors

ISSN: 2394-3114
Vol-40-Issue-68-March-2020

terrorism. Barry Collin credited for attributing the term "cyber terrorism", who coined the term in the year 1997.[4]

We are living in a society that is increasingly dependent upon information technology. The technology can deliver a number of benefits; it also introduces new vulnerabilities that can be exploited by persons with the necessary technical skills. Nowadays technology is increasingly seen as potential tool for terrorist organizations. This is leading to the emergence of a new threat in the form of 'cyber terrorism', which attack technological infrastructures such as the internet in order to help further their cause. The traditional concepts and methods of terrorism have taken new dimensions, which are more destructive and deadly in nature. In the age of information and communication technology terrorists have acquired an expertise to produce the most deadly combination of weapons and technology, which of not properly safeguard in due course of time, will take its own toll. The damage so produced would be almost irreversible and most catastrophic in nature. In short, we are facing the worst form of terrorism popularly known as cyber terrorism. It is said 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.

Information technology 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'. "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 asset 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.[5]

The face of global terrorism is changing at a rapid pace. While the motivations remain the same, we are now faced with new and unfamiliar weapons. The intelligence systems, security procedures, and equipment that are meant to protect us, are now powerless against this new devastating weapon, called cyber terrorism. Furthermore, the methods of counter terrorism that our world relies on are becoming somewhat obsolete because this enemy does not attack us with explosives but this enemy attacks us with computer viruses and seeks to disrupt our computer systems which we have become so reliant on. 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.

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. • Physical Attack: The computer infrastructure is damaged by using conventional methods like bombs, fire etc. • 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. • 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 user's knowledge in order to induce errors, [6] terrorists' can also use the Internet for organisational purposes rather than to commit acts of terror like; propaganda, information gathering, preparation of real-world attacks, publication of training material, communication, and terrorist financing. This means that organisations or governments which depend on the operation of computers and computer networks can be easily attacked.[7]

Terrorism even today continues to challenge the peace and stability of our modern society. It challenges the notion of peace and security in the minds of people, society, government and world. Despite

Copyright © 2020 Authors

ISSN: 2394-3114
Vol-40-Issue-68-March-2020

measure taken by the governments and law enforcement agencies, terrorism continues to echo and haunt with the emotions of fear, insecurity and anxiety.

TOOLS OF CYBER TERRORISM

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

1. 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 outflow facilitates hacking.
2. Trojans: Programmes which pretend to do one thing while actually they are meant for oozing something different, like the wooden Trojan Horse of the 1st Century BC.
3. Computer Viruses: It is a computer programme, which infects other computer, programmes by modifying them. They spread very fast.
4. 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.
5. 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.
6. Denial of Service: These attacks are aimed at denying authorized persons access to a computer or computer network.
7. 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.

6. CYBER CRIME/ TERRORISM AND INDIA'S NATIONAL SECURITY

Cyber crime also called computer crime. The use of a computer as an instrument to promote illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities or violating privacy. Cybercrime, especially through the internet, has grown in importance as the computer has become central to commerce, entertainment, and government. Cyber crime means any criminal or other offence that is facilitated by or involves the use of electronic communications or information system, including any device or the internet or any one or more of them. Cybercrime can be defined as criminal activity done using the computer and the internet. This includes anything from stealing millions of rupees from an online bank account to creating and distributing virus on the computer network or posing confidential data of the business and the government on the internet. Cyber crime mainly targets computer network or devices. These types of crimes include viruses and denial of service (DoS) attacks. Computers networks are also being used for the purpose of criminal activities like stalking, identity theft or carrying out terrorist attacks. Cybercrimes incorporate harassment to an individual through internet by sending e-mail and spam messages, trafficking, posting and dissemination of obscene material including pornography and indecent exposure. Cybercrimes are also committed against all forms of property; these crimes include computer vandalism (destruction of others' property), transmission of harmful programmes and viruses or controlling and damaging computer networks.[8]

The cyberspace is being used by individuals and terrorist to threaten the international governments as also to terrorize the citizens of a country. This crime manifests when an individual "cracks" into a secure government website or military maintained website and causes damage to critical infrastructure. Smart Cities emerge from innovations in information technology and they create new economic and social opportunities. Humans are already connected via smart phones and gadgets; security devices are being used in many cities. Homes, cars, public venues and other social systems are now well connected through internet. Standards are evolving for all of these potentially connected systems. They will lead to unprecedented improvements in the quality of life. To benefit from them, city infrastructures and services are changing with new interconnected systems for monitoring, control and automation.

Copyright © 2020 Authors

ISSN: 2394-3114
Vol-40-Issue-68-March-2020

Intelligent transportation, public and private, will access a web of interconnected data from GPS location to weather and traffic updates. Integrated systems will aid public safety, emergency responders and in disaster recovery. Two important and entangled challenges are: security and privacy. Security includes illegal access to information and attacks causing physical disruptions in service availability. As digital citizens are more and more instrumented with data available about their location and activities, privacy seems to disappear. Privacy protecting systems that gather data and trigger emergency response when needed are technological challenges that go hand in hand with the continuous security challenges. Their implementation is essential for a Smart City in which we would wish to live. [9]

Cyber terrorism is the latest contribution of the twenty first century. It is causing increasingly serious risks to the economy as well as to national security. They are now widely accepted in the international community as a top-tier risk, if not the most pertinent risk, to national security. Janet Napolitano, Secretary of the Department of Homeland Security (DHS) recently stated that, "**cyber-terrorism now tops the list of security concerns**."[10] In 1948, Hans Morgenthau wrote that national security depends on the integrity of a nation's borders and its institutions. However in 2016, everything from elections to electricity, are computerized and connected to the Internet, the terrestrial distance between adversaries can be irrelevant because everyone is a next-door neighbor in cyberspace. The next wave of national security threats, therefore, might originate from cyberspace. It is a complex and multidimensional problems against which no degree of technical superiority is likely to suffice. In the current security scenario cyber terrorism is an emerging threat for India's national security where, several security establishments, business firms and national assets become vulnerable targets. As the cybercriminals, 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 antinational 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 Nowadays, the cyber net is 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 security challenges in the country. In the last one decade, cyber threat has emerged as a key ingredient in a nation's arsenal to protect itself against onslaught of its enemies. Counter cyber security force is the fifth wing after Army, Navy, Air Force and Space, whose main task is to protect the sovereignty, integrity and national security of a Nation-State from external enemies. No nation may feel secure, if it is not having a well defined cyber security agenda in place. This potential threat of cyber terrorism can be realized in the words of former Home Minister Mr. P. Chidambaram at a meeting of National Counter Terrorism Center (NCTC) held on 5th May, 2012: "There are terrorists' threats in the cyber space, which is the fifth domain after land, sea, air and space. Much of our critical infrastructure lies in the cyber space. Cyber crimes such as hacking, financial fraud, data theft, espionage ete would have in certain circumstances, amount to terrorist acts."[11]

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 and indulged their activities by using social networks to wide spread harm and distress among the communities

Copyright © 2020 Authors

ISSN: 2394-3114
Vol-40-Issue-68-March-2020

It brought the local communal issue in to national hemisphere with international ramification. The investigation revealed the role of Pak based terrorists groups to sensationalize the issue of local communal violence in Assam in to country wide aggression by spreading rumors' and fake news through internet. It led mass exodus of people belonging to North east from major Indian cities following the rumors' of possible attack on them. [12]

The widespread use of social networks by the terrorist groups arose to 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. [13]

CONCLUSION

The consequences of global networks and communications are both constructive and troublemaking, raising new opportunities and challenges for individual, national and international stability. As a result of networks, modern war is practically based on cyber platform where it has shown how cyber attackers use same old camouflage theory and techniques to apply in virtual battle ground i.e. internet and achieve target without getting captured or attacked. War in today's time after the involvement of Computer is not limited to direct, limited or total war; it has now become all time war and where citizens, businesses, military are made their target. Waging styles of war has changed due to evolution of time but its root remains same with basic principles being unchanged where for destabilizing a nation, its citizens are made target as targeting population compels the target nation to surrender because citizens by then rise in revolt against Government for failing to provide security. Cyber war surely going to be the field of all future wars where nations will develop more ways to integrate cyber into physical arena by inducting more weapons like laser or electromagnetic into its arsenal as strike weapon than nuclear weapons. The WiFi waves are used to download songs or videos and attackers are trying to install backdoor in system and will focus on damaging more physical resources and persons like that of increasing speed of CPU fan thereby causing huge harm to human life. Improvised techniques might also add in exploding of battery by manipulating codes or sometimes by generating a reflex action i.e sending back same amount of energy to the socket or main line causing chance of power shock to human or sometimes sending huge wavelength of sounds to human ears when headphone is connected making virtual contract killing quiet possible. Days are near when computer virus will not only limit itself to infecting systems but to go on for preying on human who are operating it as this can be very well possible if genius brains(hackers) in cyber world comes with combinations of chains carried out in systematized channel.

If India fails to take this threat seriously we are in jeopardy of a digital Pearl Harbor and open ourselves up to a repeat of the past terrorist attack. If we continue to question whether this threat is viable and do nothing about it we are vulnerable to an attack. The threat of cyber terrorism may be exaggerated and manipulated, but we can neither deny it nor dare to ignore it. Thus, India must consider cyber security as an essential component of national security and foresee and plan for various challenges arising out the growth of the internet and digitalization of governance. In order to fight cyber terrorism, a lot of effort should be done at the personal level, the country level, the regional level, as well as the international level to fight against this transnational type of crime.

With the rapid march of technology, cyber attacks will only become more widespread as the use of internet for manipulating things increases. We have now entered into a new phase of conflict in which cyber weapons can be used to create physical destruction in someone else's critical infrastructure. And there is a distinct possibility that the disruptions and dislocations it causes are permanent and sever.

Copyright © 2020 Authors

ISSN: 2394-3114
Vol-40-Issue-68-March-2020

FOOT NOTES

1. Gautam Sen (Ed) Introduction , National Security , (NISDA, Pune, 2006) pp.vi-vii
2. Archana Upadhya and Abu Nasar Saied Ahmed , "Redefining National Security: An Overview in Abu Nasar Saied Ahmed (Ed) (Akansha Publishing House, New Delhi, 2007), pp.17-37
3. P. A. Ghosh, Conceptualizing National Security, DAKSH Vol 17, 2019,PP. 7-9
4. 1. Cyber Terrorism - How Real is the Threat? (2016, May 4). Retrieved 4 August 2019,from https://www.checkmarx.com/2016/05/04/cyber-terrorism-real-threat-2/
5. Col. S S Raghav (2010), "Cyber Security In India's Counter Terrorism Strategy", retrieved from URL: http://ids.nic.in/art_by_offids/Cyber%20security%20
6 John Fay, Encyclopedia of Security Management, 2 nd edition, Butterworth and Heinemann, UK, 2007, p. 529
7. What is cyberterrorism? - Definition from WhatIs.com. Retrieved 1 August 2019, fromhttps://searchsecurity.techtarget.com/definition/cyberterrorism
8. http//www.idsa.-india.org/an-apr9-9.html
9. Akhgar, B., & Brewster, B. (2016). Megatrends and Grand Challenges of Cybercrime and Cyberterrorism Policy and Research.In Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities.p. 5-6. Basingstoke, England: Springer.
10. http://www.satp.org/satporgtp/sair/Archives/sair10/10_48.htm#assessment1) and mha.nic.in/pdfs/HM-OpenStat-050512.pdf
11. Dr Omair Anas (2015), "In search of India's Cyber Security Doctrine", ICWA Policy Brief, New Delhi.
12. F Cassim (2012), "Addressing the Specter of Cyber Terrorism: A Comparative Perspective", Retrieved from URL: http://www.saflii.org/za/journals/ PER/2012/27.html
13 http://dspace.cigilibrary.org/jspui/bitstream/123456789/15033/1/Cyberterrorism%20How%20Real%20Is%20the%20Threat.pdf?1

Copyright © 2020 Authors