Dimensions of Cyberterrorism: An Overview*

S.Ramdoss**

1. Introduction

There is a tendency among human beings to use and/or abuse things whether it's territory or technology. In this way, the advent of information technology is being exploited by the non-state actors or the terrorists. It is said that the measure of conventional terrorism and its impacts are more or less on par with the cyberterrorism and its impact. More particularly, the psychological damage on the victims is something that needs to be addressed by the policy makers sooner than later. On the other hand, it is also imperative to look into why they (terrorists) indulge in destructive activities. Studies and research works on the issue of terrorism attribute several contributing factors which either push or pull gullible individuals to the acts of violence and extremism. However, unlike conventional terrorism the phenomenon of cyberterrorism has not caused much havoc among the general public. This probably, could be one of the reasons why the impact or consequences of cyberterrorism on the victims are given the least importance. The non-state actors are largely exploiting the internet and social media, *inter alia*, for propaganda, financing, radicalization and recruitment. It is imperative to protect the critical information infrastructures from the probable cyber attacks from the terrorist organizations.

The need for critical infrastructure protection is producing international cooperation and international law. Regional organizations, such as ASEAN, the European Union (EU), and the Organization of American States (OAS), and security regimes, such as the North Atlantic Treaty Organization (NATO), promote cooperation on critical infrastructure protection. Within treaties that address critical infrastructure sectors – such as civil aviation, maritime transport and nuclear safety – international organizations are paying more attention to cyber security. States in different geographical and political contexts are using international legal instruments to increase protection of cyber-enabled critical infrastructure (Fidler, 2016).

---

* Revised version of the paper presented at the Indian Institute of Advanced Study (IIAS), Shimla.

** UGC – IUC Associate, IIAS, Shimla.

Definition of the concepts

The phenomenon of terrorism could be described simply as the use or threat of violence, calculated to create an atmosphere of fear and alarm and thereby to bring about some political result (Jenkins, 1992).

The Global Terrorism Index (2017) defines terrorism as "the threatened or actual use of illegal force and violence by a non-state actor to attain a political, economic, religious, or social goal through fear, coercion, or intimidation"

Cyberterrorism is the convergence of terrorism and cyberspace. It means unlawful attacks and threats of attacks against computer networks, and information stored therein to intimidate or coerce a government or its people in furtherance of political or social objectives (Paylee, 2015).

2. Magnitude of the Problem

There is a growing tendency among the terrorists to exploit the information technology particularly the internet and the social media to advance their ideology.The terrorist organizations resort to different forms of terrorism according to the prevailing conditions and the capabilities they possess. However, in the current era of digital technology, the internet and social media are widely exploited by the terrorist organizations across the globe. Hence, it is inevitable for any extremist organizations to exploit the internet and social media.

Dutt (2017) stated that as cyberspace expands and evolves, cyber-threats continue to escalate in sophistication and magnitude. While the internet has ushered in a new era of socio-economic development and prosperity, it has also created easy and low-risk opportunities for non-state actors or terrorist organizations to amplify their operations. Cyber attacks targeted at critical information infrastructures can potentially devastate a country's economy and threaten public safety.

Pathak (2016) observed that a paradigm shift that the 'Age of information' is creating is connected with the rise of asymmetric war as a new kind of combat that used terrorism as its instrument. the new global terror created by Islamic radicals represented by the ISIS in Syria and Iraq and by the regrouped Al Qaeda – Taliban combine in the Pakistan-Afghanistan belt is

taking on the US-led West, the Shiites and idol worshippers – in that order – and has spread across international boundaries. It has produced the ultimate weapon in the form of an individually indoctrinated suicide bomber who can inflict unacceptable destruction of strategic targets and human population and render conventional armies ineffective. this threat can be handled only through intelligence that is now required to trace out even the 'lone wolves' on the basis of detection of covert communications, training modules and transfer of funds. The sleeper cells offer the same challenge to the intelligence agencies. The author argued that a new level of coordination in exchange of information and action is required in which intelligence coming top down from national intelligence set up and intelligence from below produced by the police, become equally important.

Conway (2006) concluded that researchers are still unclear whether the ability to communicate online worldwide has contributed to the increase in terrorist violence. It is agreed, however, that online activities substantially improve the ability of such terrorist groups to raise funds, lure new faithful and reach a mass audience. The most popular terrorist sites draw tens of thousands of visitors each month. Obviously, the internet is not the only tool that a terrorist group needs to 'succeed'. However, the internet can add new dimensions to existing assets that groups can utilize to achieve their goals as well as providing new and innovative avenues for expression, fund raising and recruitment.

The number of incidents of cyberterrorism reported in India for the last few years indicates that the issue of cyberterrorism has not assumed serious proportion yet. According to the Reports of Crime in India, 2015 and 2016 the following number of cases was registered under cyberterrorism in the last couple of years: 2014 (5 cases); 2015 (13 cases) and 2016 (12 cases).

3. Forms of Cyber attacks

Some of the most common forms of cyber attack being carried out by the perpetrators who are members of the terrorist and /or criminal syndicates have been presented here:

Hacking

The most popular method exploited by the terrorist organizations around the world. The perpetrators gain unauthorised access to a computer or a network of computers.

Trojans

The programmes which pretend to do one thing while actually they are meant for doing something different.

Computer Virus

It is a computer programme which infects other computer programmes by modifying them. It spreads very fast.

Computer Worms

It is a self-contained programme or a set of programmes that is able to spread functional copies of itself or its segments to other computer systems usually via network connections.

E-mail related attack

Generally, worms and viruses have to attach themselves to a host programme to be injected. Certain e-mails are used as host by virus and worms.

E-mails are also used for spreading disinformation, threats, and defamatory stuff.

Denial of Service (DoS)

These attacks are aimed at denying authorised persons access to a computer or computer network(Paylee, 2015).

4. The Exploitation of Internet

The exploitation of the internet by the terrorist organizations is rampant nowadays. The cheap, accessible and multipurpose nature of the internet enables the perpetrators to resort to such technology to augment their activities. The terrorists exploit the internet and social media mainly for;*inter alia*, communication, recruitment, indoctrination/radicalization, propaganda, fund raising and information gathering.

Weimann (2004) identified eight major ways in which terrorists currently use the internet. These are psychological warfare, publicity and propaganda, data mining, fund raising, recruitment and mobilization, networking, information sharing and planning and coordination.

Conway (2006) also stated that terrorists can also use the internet as a tool of psychological warfare through spreading disinformation, delivering threats and disseminating horrific images. The author further observed that until the advent of the internet, terrorists' hopes of winning publicity for their causes and activities depended on attracting the attention of television, radio, or the print media. Moreover, the internet offers terrorist groups an unprecedented level of direct control over the content of their messages.

Fidler (2016) argued that within high-tech terrorism, cyber technologies are distinct because they are: more accessible, cheaper, less risky and more malleable than nuclear, biological and chemical materials and offer ways to attack across a spectrum of consequences, gather intelligence, communicate in planning and conducting operations, spread propaganda, engage in 'virtual' criminal activities and raise financial resources.

The cyber space has opened up a new kind of combat called the asymmetric warfare in which the forces behind global terror use the sophisticated technology and IP software for fund transfer, spread of subversion and recruitment of agents and foot soldiers (Pathak, 2016).

According to Conway (2006), terrorists seek financing both via their websites and by using the internet infrastructure to engage in resource mobilization using illegal means. Further, the author elaborated that numerous terrorist groups request funds directly from web surfers who visit their sites. Such requests may take the form of general statements underlining the organizations need for money, more often than not, however, requests are more direct urging supporters to donate immediately and supplying either bank account details or an online payment option.

Conway (2006) argued that the internet has the ability to connect not only members of the same terrorist organization but also members of different groups. there are a number of websites available that express support for terrorism. These sites and related forums enable terrorists to exchange not only ideas and suggestions, but also practical information about how to build bombs, establish terror cells and ultimately perpetrate attacks.

As stated elsewhere, recruitment is one of the major works of the terrorist organizations for which the internet is largely exploited by the terrorist groups. Recruitment refers to the terrorist groups' efforts to recruit and mobilise sympathisers to more actively support terrorist activities. The web offers a number of ways for achieving this: it makes information gathering easier for potential recruits by offering more information, more quickly and in multimedia format; the global reach of the web allows groups to publicise events to more people and by increasing the possibilities for interactive communication, new opportunities for assisting groups are offered along with more chances for contacting the group directly (Conway, 2006).

Cell phones, internet, social media and transport connectivity are extensively used by insurgent groups, terrorists and transnational criminal organizations to coordinate their activities across the globe, and promote their political and economic interests (Srikanth, 2016).

Conway (2006) pointed out that one of the major uses of the internet by the terrorist organizations is thought to be information gathering. The author elaborated the two issues pertaining to the information gathering by the terrorists. The first may be termed as 'data mining' and refers to terrorists using the internet to collect and assemble information about specific targeting opportunities. The second issue is 'information sharing', which refers to more general online information collection by terrorist organizations.

5. The Profile of the Terrorists

By and large, the characteristics of the terrorists are said to be similar in terms of their socio-economic backgrounds, the kind of political economic structure etc. The terrorists indulge in various forms of destructive activities. While many factors appear to be almost the same for both the conventional terrorists and those involve in cyberterrorism, the technological skills keep the cyberterrorists apart from the conventional or kinetic terrorists.

Demographic profile

According to the Global Terrorism Index (2017), there are multiple paths to radicalization and individuals can exhibit both high and low levels of education, income, religious or political knowledge. The GTI further stated that relative deprivation can also be a driver of terrorist recruitment as it leads to the creation of an 'us vs them' attitude.

According to Jenkins (1992), many of the terrorists have been urban middle class and upper class (not economically deprived); males in their early twenties; with University or at least secondary school education.

Common Psychological features

According to Behavioural Analysts, the terrorist appeared to be a person who is: Narcissistic; emotionally flat; easily disillusioned; incapable of enjoyment; rigid; and a true believer who is action-oriented and risk seeking.Psychiatrists could label terrorists as: Neurotic; Possibly Sociopathic; and not clinically insane (Jenkins, 1992).

6. The Impact

The impact or consequences of cyberterrorism need to be measured, analyzed and evaluated. Only a very few studies have been conducted to measure the impact of cyberattacks or cyberterrorism on the non-combatants or the civilians. The cyberterrorism has the potential to stifle the financial transactions and the critical information infrastructures in the country.

According to Jenkins (1992), Public opinion polls, along with measurable decisions like not flying or avoiding certain countries provided the measure of effect.As stated by Jenkins, the impact of cyberterrorism is also equally capable of creating such threat perceptions among the masses. This is more likely when the cyberattacks or threats of cyberterrorism are on the critical information infrastructures.

Gross et al (2017) through empirical studies suggest the effects of cyberterrorism track those of conventional terrorism. Overall, experimental subjects exhibit marked signs of stress, personal insecurity and heightened perceptions of cyber threat. They further stated that cyberattacks cause stress, anxiety and insecurity. Threat perception rises to a level very close to conventional terrorism when cyberterrorism turns deadly. Through empirical evidence the authors demonstrate

how cyberterrorism, like conventional terrorism, impairs psychological well-being and increase perceptions of threat.

Many people, particularly those with high levels of threat perception, are willing to support strong government policies. These policies split along two lines and include foreign policy (e.g. cyber/and or kinetic military responses to cyberattacks) and domestic policy (e.g. tolerance of government surveillance and control of the internet). As threat perception increases, individuals take increasingly stringent political views. Like conventional terrorism, cyberterrorism hardens political attitudes as individuals are willing to exchange civil liberties and privacy for security and support government surveillance, greater regulation of the internet and forceful military retaliation in response to cyberattacks (Gross et al, 2017).

Paletta (2015) stated that fear of terrorist cyber attacks has grown as dependence on Information Communication Technologies (ICTs) deepened and as the skills and means to launch such attacks disseminated. However, Canetti et al (2016) argued that despite its growth, cyberterrorism unlike conventional terrorism does not threaten life and limb. As a result, very little attention is paid to the effects of cyberterrorism on civilians.

Gross et al (2017) stated that while not all the perpetrators or their goals are immediately obvious, they do not appear motivated by monetary gain. Rather it seems that they aim to impair public confidence, disrupt civil society and seed anxiety and insecurity by crippling digital and financial resources, undermining the institutions of governance and disrupting social networks.

Gross et al (2017) revealed through empirical works that threat perception, not an actual attack is sufficient to unsettle individuals to the extent many terrorists desire. as a result, authorities will need to recognize that they cannot reduce fears of cyberterrorism and its pervasive effects solely by eliminating cyberattacks that will, quite possibly, only grow more severe.

7. The Information Technology Act, 2008

The Act that deals with cyberterrorism in the context of India is the Information Technology (Amendment) Act, 2008 which is an amended version of the Information Technology Act, 2000. Some of the salient features of the Information Technology (Amendment) Act, 2008 have been reproduced here:

Section 66 F deals with cyberterrorism and this section defines what cyberterrorism is and also prescribes the punishment for the offence of cyberterrorism.

Section 66 F (1) Whoever –

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

i) denying or cause the denial of access to any person authorised to access computer resource; or

ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or

iii) introducing or causing to introduce any computer contaminant,

And by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70; or

(Critical Information Infrastructure means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety)

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise,commits the offence of cyber terrorism.

(2) whoever commits or conspires to commit cyberterrorism shall be punishable with imprisonment which may extend to imprisonment for life.

Section70A deals with the National Nodal Agency for the protectionof the Critical Information Infrastructure (CII).

Section70B deals with the Indian Computer Emergency Response Team (I-CERT) and this serves as the National Nodal Agency for the protection of the Critical Information Infrastructure.

Functions of ICERT

The key functions of the Indian Computer Emergency Response Team (I-CERT) are as follows:

1. Collection, analysis and dissemination of information on cyber incidents.

2. Forecast and alerts of cyber security incidents.

3. Emergency measures for handling cyber security incidents.

4. Coordination of cyber incidents response activities.

5. Issue guidelines, advisories, vulnerability notes and white papers relating to Information

Security practices, procedures, prevention, response and reporting of cyber incidents.

However, Jajodia and Krishnaswamy (2017) observed that the CERT-In does not do its job very well. It is also charged with safeguarding and monitoring the country's critical digital infrastructure. But, the public do not know what it does because it neither reports incidents, nor publishes an analysis of the incidents.

8. Conclusion and Suggestions

The exploitation of the internet and social media by the terrorists are growing leaps and bounds to facilitate their extremist activities.The opportunities are abundant in the information superhighway to unleash violence and hatred and extremism through hate speech, horrific images and videos, provocative texts and so on and so for.

This paper argues that instead of focusing only on counter-terrorism efforts in terms of sophisticated weapons, arms and ammunitions, the focus must be on alleviating the root causes of terrorism. The root causes are more likely to lead to the socio-economic aspects of human life that pave way for alienation, relative deprivation etc.

This paper firmly believes that the best counter-terrorism strategy is to genuinely address the socio-economic issues surrounding the vulnerable groups. If this is addressed properly, then that is a heavy blow to the recruitment and radicalization and vice-versa. This strategy will certainly take time but the outcome will be positive and long lasting for a peaceful and harmonious society at large. Furthermore, this strategy will demoralize the non-state actors' plan of radicalization and recruitment.

To achieve such a peaceful and harmonious society, the efforts of government and civil society should go hand in hand in addressing social maladies at the grassroots itself. Because, there is a greater likelihood that the social disorders, crimes eventually lead to greater risks of large scale violence, extremism and terrorism. Hence, sincere and timely efforts of the stakeholders will definitely prevent and contain the menace of terrorism in all its forms.

Suggestions

The root causes of terrorism must be identified and addressed appropriately.it is prudent to be proactive than reactive.

There should be local, national, regional, and global level cooperation and coordination to address the issue of various forms of terrorism.

There is a pressing need to create a greater awareness and sensitization among the youth about the negative impact of terrorism in general and cyberterrorism in particular.

The growing nexus between terrorist organizations and transnational criminal syndicates must be curtailed.

The cyber security skills and training should be imparted widely as the digital drive is gaining momentum; it is indispensable to protect the general public from the victimization in cyber space.

References

Canetti D, Gross ML, Waismel-Manor I. (2016). Immune from Cyber-Fire? The Psychological & Physiological Effects of Cyberwar. In Allhoff F, Henschke A, and Strawser BJ (eds). *Binary Bullets: The Ethics of Cyberwarfare*. Oxford: Oxford University Press. pp.157- 176.

Conway, Maura (2006). Terrorism and the Internet: New Media – New Threat. *Parliamentary Affairs*. Vol59.No.2. pp. 283-298

Crime in India (2015 and 2016). The National Crime Records Bureau, Ministry of Home Affairs, Government of India.

Dutt, Shekhar (2017). Aspects of Security in Cyber Space. *Chanakya Journal of CCSS.* Vol.2 (1). December 2017 pp. 49-53.

Fidler, David P. (2016). Cyberspace, Terrorism and International Law. *Journal of Conflict&Security Law.* Vol.21 No.3. pp.475-493.

Gross, ML, Canetti, D, Vashdi, DR. (2017).Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes. *Journal of Cybersecurity*. 3(1).pp.49-58.

Jajodia, Nirmalendu and Krishnaswamy, Arvind (2017). A Cashless Society, Cyber Security and the Aam Aadmi. *Economic & Political Weekly*. Vol.52 No.14. 8 April 2017

Jenkins, Brian Michael (1992). Terrorism. In *Encyclopedia of Sociology.* Edgar F.Borgatta and Marie L. Borgatta (eds.). Vol.4. pp.2168- 2171.New York: Macmillan Publishing Company.

Paletta, D. (2015). 'FBI Director Sees Increasing Terrorist Interest in Cyberattacks against U.S.' *Wall Street Journal*. New York City, 22 July 2015

Pathak, D.C. (2016). Age of Intelligence.*Chanakya Journal of CCSS*. Vol.1 (1). September 2016 pp. 11-16.

Paylee, S.N. (2015). Cyber Security in India Implications for Foreign Policy. New Delhi: Sumit Enterprises.

Srikanth, H. (2016). Combating Transnational Crimes in the Era of Globalization: Strategies for India and the ASEAN. *International Studies*. 53 (2).pp. 91-104.

The Global Terrorism Index (2017). The Institute for Economics and Peace: Sydney.

The Information Technology (Amendment) Act, 2008.

Weimann, G. (2004). How Modern Terrorism Uses the Internet. United States Institute of Peace.pp.5-11.