Available online at www.elixirpublishers.com (Elixir International Journal)

International Law

Elixir Inter. Law. 40 (2011) 5538-5544

ISSN: 2229-712X

Digitalized terrorism -the technological advancement of crime

Nidhi Saxena[1] and Priti Saxena[2]

[1]Faculty of Law, Mody Institute of Technology and Science, Laxmangarh, Sikar, Rajasthan

[2]Department of Human Rights, School for Legal Studies, Babasaheb Bhimrao Ambedkar University, Lucknow (U.P.).

ARTICLE INFO

Article history:

Received: 26 August 2011;

Received in revised form:

10 November 2011;

Accepted: 22 November 2011;

Keywords

Terrorism,
Digitalized terrorism,
Cyberterrorist,
Digitalizedterrorism,
Terrorists Attacks,
Netizens.

ABSTRACT

'The start of new century may have seen a decline in the number of incidents of 'traditional' terrorism such as hijackings and kidnappings but the lethality of the terrorist potential has risen to a frightening degree with the advent of digitalized terrorism , and its links to computer technology. The vulnerability of the critical infrastructure has led to increasing concern that it will be the target of terrorist attacks. In this highly topical study the authors examine the new terrorist tools and their appalling capacity for the destruction of human systems. The authors claim that the technological revolution has effectively 'democratized' computer knowledge so that the forces of law and order no longer have an inherent advantage of power and privilege. Their special challenge in the new century will be to match the resourcefulness and ingenuity of their terrorist adversaries. The purpose of this paper is to explore how the Internet is altering the traditional concept of terrorism. What are the common Ways of terrorists attacks Cyber-terrorism or digitalized terrorism is a catastrophic phenomenon that has not yet attracted the attention of the Indian Legislature exhaustively. The paper consider whether there is a need to react to digitalized terrorism and if so, to what extent?

© 2011 Elixir All rights reserved.

Introduction

The growing dependence of our societies on information technology has created a new form of vulnerability. The traditional concepts and methods of terrorism[1] have taken new dimensions, which are more destructive and deadly in nature. In the age of information technology the terrorists have acquired an expertise to produce the most deadly combination of weapons and technology, which if not properly safeguarded in due course of time, will take its own toll. The damage so produced would be almost irreversible and most catastrophic in nature.[2] To be ignorant towards cyber-Terrorism /digitalized terrorism ,, will be such as giving terrorists the chance to approach targets that would otherwise be utterly unassailable, such as national defense systems and air traffic control systems. To be ignorant towards new digitalized terrorism, will be such as giving terrorists the

[1]Terrorism is an old phenomenon. The first words come from the beginning of first century after Christ, when Romans ruled Palestine, and a Jewish order called the *Zealots* committed disastrous revolt that ended in the mass suicide. During 1090-1275, a Shiite Muslim sect, *Assassins*, tried to purify Islam using drug hashish and killing their Sunni rivals. But, the word *terrorism* comes from the French Revolution (1793-1794), when terror was used by the state as a mean to eliminate counterrevolutionary elements.(**see** Professor Dumitru OPREA, PhD"Alexandru Ioan Cuza" University of Iasi, The Information System and the global terrorism, available at ssrn.com) accessed on 20/10/09

The definition of "terrorism" has been well studied, defined, and documented. As per Traditional definition of terrorism

"It is an act or aggregation of premeditated acts involving criminal violence, intending to intimidate civilian population and coerce governmental decision-making, or, generally, to express disagreement for governmental policies and actions". The basic characteristic of terrorism is the use or threat of violence against persons or property aiming to cause enough harm to attract attention, generate fear, and affect decision-making. Unlike conventional crime, it has its roots on strong ideology, it is basically an effort designed to impose it by illegal and violent means.(See Varvara Mitliaga, Digitalized terrorism : a call for Governmental Action?, available at http://www.bileta.ac.uk/document%20library/1/digitalized terrorism %20-%20a%20call%20for%20governmental%20action.pdf) accessed on 22/10/09

One of the enduring axioms of terrorism is that it is designed to generate publicity and attract attention to the terrorists and their cause, media publicity is indispensable for an attack to be successful and attain its scope. Furthermore, attacks are always premeditated and carefully planned. Terrorists act either nationally or internationally, especially after the development of telecommunication and transportation.

The FBI definition of terrorism- "The unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives".

Department of State definition of terrorism defined the term as "Premeditated politically motivated violence perpetrated against noncombatant targets by sub-national groups or clandestine agents".

[2]Praveen Dalal, Cyber , and its solutions: an Indian perspective available at http://www.naavi.org/praveen_dalal/pd_cyber_terrorism_oct25_04_02.htm, accessed on 22/3/09

Tele:

E-mail addresses: nidhisaxena.law@gmail.com

© 2011 Elixir All rights reserved

chance to approach targets that would otherwise be utterly unassailable, such as national defense systems and air traffic control systems.

The more technologically developed a country is, the more vulnerable it becomes to cyber attacks against its infrastructure. In short, we are facing the worst form of terrorism popularly known as "cyber-terrorism or digitalized-terrorism"[3]. The expression "cyber-terrorism or digitalized-terrorism, " includes an intentional negative and harmful use of the information technology for producing destructive and harmful effects to the property, whether tangible or intangible, of others[4]. Why would a terrorist decide to use the Internet, rather than using the usual methods of assassination, hostage taking and guerrilla warfare? element of the problem is that terrorist may come to realize that removing one official from office only causes another to take the officials place, which may not cause the result the terrorist wished to achieve. By using the internet the terrorist can affect much wider damage[5] or change[6] to a country than one could by killing some people. From disabling countries military defenses to shutting off the power in a large area, the terrorist can affect more people at less risk to him or herself, than through other means.

The laws of India have to take care of the problems originating at the international level because the Internet, through which these terrorist activities are carried out, recognizes no boundaries. Thus, a cyber terrorist can collapse the economic structure of a country. India may not have any reciprocal arrangements, including an "extradition treaty". The only safeguard in such a situation is to use the latest technology to counter these problems. Thus, a good combination of the latest security technology and a law dealing with cyber-Terrorism /digitalized terrorism is the need of the hour.[7]

The threat posed by cyber-Terrorism /digitalized terrorism has grabbed the attention of the mass media, the security community, and the information technology (IT) industry, Despite all the gloomy predictions of a cyber-generated doomsday, no single instance of real cyber-Terrorism /digitalized terrorism has been recorded[8] most critical infrastructure in Western societies is networked through computers, the potential threat from cyber-Terrorism /digitalized terrorism , is, to be sure, very alarming. Hackers, although not motivated by the same goals that inspire terrorists, have demonstrated that individuals can gain access to sensitive information and to the operation of crucial services.[9]

---

[3]The definition of "Cyber terrorism," cannot be made exhaustive as the nature of crime is such that it must be left to be inclusive in nature. The nature of "cyberspace" is such that new methods and technologies are invented regularly; hence it is not advisable to put the definition in a straightjacket formula or pigeons hole. (See Praveen Dalal " *Cyber Terrorism and its solutions: an Indian perspective* , Available at http://www.naavi.org/praveen_dalal/pd_cyber_terrorism_oct25_04_02.htm) accessed on 22/3/09

Also, The U.S. National Infrastructure Protection Centre defined the term as "A Criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence , destruction and /or disruption of services to Create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to particular political, social or ideological agenda".

But another opinion regarding the term Cyber- terrorism , is given by Dorothy E. Denning,(*Cyberterrorism* -Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, US House of Representatives, 23 May 2000, available at<http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>. accessed on 24/10/09) is " not any malicious use of information technology constitutes cyber-terrorism. Cyber-terrorism is quite a new term, used to describe the convergence of terrorism and cyberspace. It is generally understood to mean attacks and threats of attack against computers, networks and the information stored therein, when done to intimidate or coerce a government or people in furtherance of political or social objectives.

[4]For instance, hacking of a computer system and then deleting the useful and valuable business information of the rival competitor is a part and parcel of cyber or digitalized terrorism.

[5]For Instance a Cyber Terrorist will disrupt the banks, the international financial transactions, the stock exchanges. The key: the people of a country will lose all confidence in the economic system. Would a Cyber Terrorist attempt to gain entry to the Federal Reserve building or equivalent? Unlikely, since arrest would be immediate. Furthermore, a large truck pulling alongside the building would be noticed. However, in the case of the Cyber Terrorist, the perpetrator is sitting on another continent while a nation's economic systems grind to a halt. Destabilization will be achieved.

[6]A Cyber Terrorist will remotely access the processing control systems of a cereal manufacturer, change the levels of iron supplement, and sicken and kill the children of a nation enjoying their food. That Cyber Terrorist will then perform similar remote alterations at a processor of infant formula. The key: the Cyber Terrorist does not have to be at the factory to execute these acts.

A Cyber Terrorist will place a number of computerized bombs around a city, all simultaneously transmitting unique numeric patterns, each bomb receiving each other's pattern. If bomb one stops transmitting, all the bombs detonate simultaneously. The keys: 1) the Cyber Terrorist does not have to be strapped to any of these bombs; 2) no large truck is required; 3) the number of bombs and urban dispersion are extensive; 4) the encrypted patterns cannot be predicted and matched through alternate transmission; and 5) the number of bombs prevents disarming them all simultaneously. The bombs *will* detonate.

A Cyber Terrorist will attack the next generation of air traffic control systems, and collide two large civilian aircraft. This is a realistic scenario, since the Cyber Terrorist will also crack the aircraft's in-cockpit sensors. Much of the same can be done to the rail lines.

A Cyber Terrorist will remotely alter the formulas of medication at pharmaceutical manufacturers. The potential loss of life is unfathomable.

The Cyber Terrorist may then decide to remotely change the pressure in the gas lines, causing a valve failure, and a block of a sleepy suburb detonates and burns. Likewise, the electrical grid is becoming steadily more vulnerable.

[7]Available at http://www.legalserviceindia.com/article/l169-Digitalized terrorism .html, accessed on 24/10/09

[8]Available at http://www.usip.org/pubs/specialreports/sr119.pdf, accessed on 24/10/09

[9]Available at http://www.usip.org/pubs/specialreports/sr119.pdf, accessed on 24/10/09

The Phenomenon of digitalized terrorism or digitalized terrorism

Computer and Internet are becoming an essential part of our daily life .The tremendous role of Computer stimulates criminals and terrorists to make it their preferred tool for attacking their target the internet. As per the definition available to qualify as digitalized terrorism, an attack[10] should result in violence against persons or property, or at least cause enough harm to generate fear. It is very difficult to exhaustively specify the structure of digitalized terrorism. The nature of cyber-Terrorism /digitalized terrorism requires it to remain inclusive and open ended in nature, so that new variations and forms of it can be accommodated in the future.

The term is considered to cover many cases of computer and internet abuse, like hacking or the dissemination of computer viruses, and generally almost any incident of an on-line based attack whose only result is nuisance and, sometimes, economic loss[11].It should be clarified, however, that the usual scope of these attacks is more for the perpetrators to test their abilities and prove to themselves and their targets that they can do it than to cause damage and inflict fear in furtherance of an ideology. The criteria for an attack to qualify as digitalized terrorism, apart from the use of information technology, are also the identity of the persons who launch it, the scope for which they do it and the result. It would be quite authoritative to consider all these bothersome attacks as digitalized terrorism, because this would automatically vest them with all the special features that the term entails, and that is certainly not the case.

Terrorists may resort to such actions in an effort to reach public opinion and make their ideas and beliefs widely known, or simply to annoy their opponents and make their existence known. That use of information technology works in the same context as using the internet to collect information about targets or to communicate and co-ordinate action with fellow conspirators or recruit supporters. Neither constitutes a complete terrorist action to qualify as digitalized terrorism. They are only an indication that, like with any other advance in technology, information technology is simply used to further unlawful purposes[12] . Digitalized terrorism then is neither a term encompassing all actual nor possible uses of information technology by terrorists, nor any disturbing abuse of computers and the internet. It is the premeditated, ideologically motivated attack against information, computer systems, computer programs, and data which result in violence and serious damage against non-combatant targets, perpetrated by persons acting in the name of an ideology with the intention to spread fear and impose their existence to the public. The pure form of cyber-Terrorism /digitalized terrorism is the use of high technology tools against high technology targets[13] .

Use of Information technology in cyber attacks

Information technology can be useful for terrorist groups in two ways:

All, computers and the internet can be used as a useful tool to enhance traditional activity.

Second, information infrastructure can constitute a new attractive target for terrorist actions.

Although these are two separate issues but they have a strong interdependence. The terrorist groups are using these two ways to enrich their activity and to cause more harm with massive fear in heart and mind of natives. The fact that terrorists may use information technology as a useful tool does not automatically mean that information infrastructure will constitute their next target, extended use and familiarization with technology, however, is a necessary step before deciding to turn against such targets. As they learn to use information technology for decision-making and other organizational purposes, they will be more likely to use it as an offensive weapon to destroy or disrupt.

The Internet as a tool

The internet can be used by terrorists as a tool in a range of ways:

They use it as a best communication medium, as electronic mail is one of the quickest, cheapest and most effective ways of contacting between any parts throughout the world.

Technology allows anonymous and secure communications & quick transfer of data, so possibility is this, that terrorists can use the internet, to exchange useful information on possible targets, like maps or instructions, and co-ordinate their action overcoming the obstacle of crossing national borders.

On internet general information for potential targets or weapons are scattered. It can be a useful resource on its own.

Anyone can maintain web pages to "advertise" their ideology disseminate propaganda and recruit supporters and same is applicable to terrorist groups also. It is the first time that they can easily reach the public directly and make their existence known in an international scale[14].

Terrorists are also said to use the internet to obtain funds.

---

[10]Attacks that disrupt nonessential services are mainly a costly nuisance would not constitute digitalized terrorism. For example, accessing remotely an air or road traffic control system and causing an accident resulting in loss of life or at least serious damage and spread of panic would constitute digitalized terrorism , while unauthorized penetration in a system aiming to distract information or simply disturb its users would not.

[11]It is not implied here that financial losses are not important,(these are important but not more than precious human life) however, they do not usually constitute the sole target of a terrorist action as they do not inflict the same fear as material damage, even more, human injury. Terrorists may of course resort to such activity in order to annoy their target and maybe steal money, but this is not a pure form of digitalized terrorism. It is rather a simple incident of criminal activity on the internet.

[12]Dorothy E. Denning, *Activism, Hacktivism, and Cyberterrorism: The Internet as a tool for influencing foreign policy*, Internet and International Systems: Information Technology and American Foreign Policy Decision making Workshop, Available at <http://www.nautilus.org/info-DIGITALIZED TERRORISM: A CALL FOR GOVERNMENTAL ACTION? Page 10 of 11 Available at http://www.bileta.ac.uk/01papers/mitliaga.html accessed on 23/10/09

[13]M. Devost, B.K. Houghton and Neal A. Pollard, *Information Terrorism: Can you trust your toaster?* Available at <http://www.terrorism.com/documents/suntzu.pdf>. accessed on 23/10/09

[14]Tom Regan, *When Terrorists Turn to the Internet*, 7/4/1999 Infowar.com, at<http://www.infowar.com/class_3/99/class3_070499a_j.shtml >. accessed on 19/10/09

Computers can be as useful for terrorists as they are for law abiding individuals as storage media or as multipurpose "machines.

These groups are also said to use strong encryption for secure communications and exchange of vital information.

Information Infrastructure as a target

The second way in which Information Technology can be useful for terrorists is by constituting their target. The terrorists use information systems to facilitate traditional forms of subversive action as an internal communication or as tools for propaganda, misinformation, recruitment and financing. The main goals of cyber terrorist attacks are to create fear and panic among civilians or to disrupting or destroying public and private assets.[15] The growing dependence of our societies on information technology means that well organized attacks to vital networks can cause incalculable damage to public or private organizations[16], and, depending on how crucial is the system, entail serious injury or damage and inflict fear to civilian population. As a result of the Internet explosion, the tools of Internet can be used as a TV or radio station, or as a support for newspaper or journal publishing without control from public authorities. In addition, chat rooms, bulletin boards or blogs are important means of communication because there is no control on the information flows.[17]It is true that dependence on information technology creates a new form of vulnerability that did not exist before and it gives terrorists the chance to approach targets that would otherwise only be a wild dream, like the manipulation of a national defence system or an air traffic control system. Astoundingly, vulnerability varies from country to country but it is analogous to technological development. The more technologically developed a country is, the more vulnerable it becomes to attacks against its infrastructure[18] . The most powerful state becomes the most vulnerable in information technology attacks. As for developing states and the third world, information technology is gradually becoming all the more important, but not yet in a degree of dependence.

So the problem has a different perspective there. There are reasons to believe that terrorist groups have the ability and the means to make extended use of technology, either as a tool or as a target.

One of the most essential features of terrorism is its strong dependence on ideology; motivation is usually strong political or religious beliefs. This entails two things: membership in terrorist groups can be, first of all, independent of social or economic status, and, secondly, irrelevant to educational or intellectual background and potential. It is very likely that terrorist groups will make increasing use of information technology given the fact that some of their members are usually well-educated individuals comfortable with the use of technology. Additionally, they have ensured financial recourses, which mean they have the means to acquire technology and "employ", if necessary, the appropriate people to use it. The use is likely to rise as terrorist groups recruit younger members that are more familiar with technology.

Furthermore, they are known to keep track of technological developments because the success of their actions partly depends on their ability to keep one step ahead of the authorities and of counterterrorist technology. Probably they would use any means available to enhance their activity.

But the transition from traditional terrorism to the use of information technology, at least as a lethal weapon, is also dependent on two other factors[19] .

First, they must understand and trust the use of the weapon. Terrorists seem to trust more easily weapons that they've built themselves or that at least have been tried by others, they usually do not seem very willing to experiment.

Second, it is also a matter of mentality; terrorists have to feel that a weapon is right for them before they use it, that it suits their ideology. A considerable number of terrorist groups seem to still like the feel of physical weapons. These are not, of course, the only decisive factors for the use of information technology and they certainly have nothing to do with using technology as a helpful tool for everyday activities. It is, however, important to keep in mind the special characteristics that differentiate terrorism from traditional crime

An overall assessment would suggest that terrorists are technologically innovative but with certain limits. Although radical in their politics, the vast majority of terrorist organizations appear to be conservative in their operations. It is not surprising that bombing is one of their favorites': it provides easy and often risk-free means of drawing attention; surreptitiously plant it, and be miles away when it explodes. To manufacture a crude bomb is not very skilled work, consequently, although it is almost certain that terrorists will make extended use of information technology as a tool, it is still debatable if they will use it as a weapon aiming at information infrastructure as a new target.

All these are possible due to the Internet services attributes like encryption, speech compression, anonymous network accounts, unknowing about content of the sites by the ISPs (Internet Service Providers). The most *dangerous cyber terrorist attacks* are those that affect the national infrastructures or businesses because the information systems have a vital role to all of them.

Ways of terrorists Attacks

The terrorist attacks that involve information system infrastructures can work in different ways, as follows[20]:

---

[15]Dumitru OPREA, PhD"Alexandru Ioan Cuza" University of Iasi, The Information System and the global terrorism, available at ssrn.com, accessed on 20/10/09

[16]Marcus Maher, *International Protection of US Law Enforcement Interests in Cryptography*,5 Richmond Journal of Law and Technology 13, (Spring 1999), p. 17, athttp://www.richmond.edu/jolt/v5i3/maher.htmlaccessed on 19/10/09

[17] Supra note 17

[18]Marcus Maher, *International Protection of US Law Enforcement Interests in Cryptography*,5 Richmond Journal of Law and Technology 13, (Spring 1999), p. 17, at<http://www.richmond.edu/jolt/v5i3/maher.html> accessed on 19/10/09

[19]John Borland, Analysing the Threat of Cyberterrorism, (interview with W. Church, founderof the Centre for Infrastructural Warfare Studies) at<http://www.infowar.com/class_3/class_3102898b_j.shtml>. accessed on 19/10/09.

[20]Denning D.E., *op. cit.*, pp. 32-37; Thomas T.L., *Al Qaeda and the Internet: The Danger of "Cyber planning"*, "PARAMETERS", US Army War College Quarterly, Spring 2003, pp. 112-123;Hennessy J.L., Patterson D.A., Lin H.S., Editors, *op. cit.*, 15-27; Fischer E.A., *Creating a National Framework for Cyber security: An Analysis of Issues and*

Service disruption Distributed denial-of-service (DDoS)[21] attacks target web sites and servers of public agencies, telephone services, transportation communication systems, utilities and the emergency-response system. This type of attacks degrades, disrupts, damages or destroys information resources so that many of activities are unable to be done. These attacks are frequently in convergence with physical ones so that important assets, including information system infrastructures, are hardly recovered and may disturb many of critical services like medical services, rescue services etc. This is made possible by first infecting several unprotected computers by way of virus attacks and then taking control of them. Once control is obtained, they can be manipulated from any locality by the terrorists. These infected computers are then made to send information or demand in such a large number that the server of the victim collapses. Further, due to this unnecessary Internet traffic the legitimate traffic is prohibited from reaching the Government or its agencies computers. This results in immense pecuniary and strategic loss to the government and its agencies. It must be noted that thousands of compromised computers can be used to simultaneously attack a single host, thus making its electronic existence invisible to the genuine and legitimate netizens and end users.

Psychological manipulation. E-mails, news or sites containing false information are used to spread terror among the population, to mobilize a group, or to diminish the credibility of public and private bodies (after the 9/11 attacks, al Qaeda ran websites to discuss the legality of the attacks. In addition, al Qaeda has several sites that offer software and programming instructions for the digital switches that run power, water, transport and communications networks. Such web sites are alneda.com, jehad.com, drasat.com, aloswa.org with feature quotes from bin Laden tape, religious legal rulings to cover his actions[22].

Capture and control. Gather of information on potential targets by stealing data, maps, diagrams and other crucial data on important facilities or network ("a Defense Department summary of the investigation said the bureau found various casings of sites nationwide. Routed through telecommunications switches in Saudi Arabia, Indonesia and Pakistan, the visitors studied emergency telephone systems, electrical generation and transmission, water storage and distribution, nuclear power plants and gas facilities"[23].

Assessing the threat posed by Cyber-Terrorism /digitalized terrorism and the general use of information technology by terrorists

There are three potential acts in cyber-Terrorism /digitalized terrorism, at the point of convergence:

- Destruction;
- Alteration; and
- Acquisition and retransmission

These three types of acts are most heinous at the point where the physical and virtual worlds converge.

Assessing the threat posed to society from pure digitalized terrorism on one hand and the general use of information technology by terrorist groups on the other are two separate issues. Both are, however, essential to examine. Deciding whether there is a need for special action will not only depend on the nature of the threat posed by pure digitalized terrorism but also on whether there is an unprecedented boost of terrorist action resulting from the use of information technology.

As for the first level of assessment, attacking vital information infrastructure could be very attractive for terrorists for several reasons. First of all, given the potential provided by computers and the internet, cyber-attacks to vital systems can be conducted remotely, anonymously and fairly cheaply, without requiring the handling of explosives or a suicide mission, which is usually a suspending factor when planning an attack. Several experts have stated that digitalized terrorism does not cause the same type of threat as nuclear, biological, or chemical threats. Many experts also believe that it would be difficult to use attacks against computers to inflict death on a large scale, and have stated that conventional physical threats present a much more serious concern for nation's security[24]. The *vulnerabilities* are increasing with spread of *Internet of things*, which can support new ways, maybe more dangerous, of terrorist attacks due to numerous facilities of things control. For instance, given the one-way trust nature of the protocols, where the Internet of things tags provides *vital information to any reader device*, there is no motivation why terrorists could not easily target

---

Options, CRS Report for Congress, February 22, 2005, http://www.acm.org/usacm/PDF/CRS_cybersec.pdf, p. CRS-7 , see Dumitru OPREA, PhD "Alexandru Ioan Cuza" University of Iasi, The Information System and the global terrorism, available at ssrn.com) accessed on 15/10/09.

[21] As per the provision of Section 43 of IT Act, 2000

"If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network -

(a) Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(b) Disrupts or causes disruption of any computer, computer system or computer network;

(c) Denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected

Here according to Explanation (i) to Section 43 of IT Act, 2000 The expression "Computer Contaminant" means any set of computer instructions that are designed -

(a) To modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or

(b) By any means to usurp the normal operation of the computer, computer system, or computer network.

Thus, distribute denial of services by the cyber terrorists will be tackled by invoking the provisions of sections 43, 65 and 66 collectively.

[22] Thomas T.L., *op. cit.*, pp. 114-115. see Dumitru "Alexandru Ioan Cuza" University of Iasi, The Information System and the global terrorism, available at ssrn.com, accessed on 23/10/09

[23]Gellman B., *FBI fears al Qaeda cyber attacks Analysts monitoring hacker activity*, "San Francisco Chronicle", June 28, 2002, p. A-1. see Dumitru OPREA, PhD"Alexandru Ioan Cuza" University of Iasi, The Information System and the global terrorism, available at ssrn.com) accessed on 15/10/09.

[24]Denning D.E., *op. cit.*, pp. 72-73.quoted by see Dumitru OPREA, PhD"Alexandru Ioan Cuza" University of Iasi, The Information System and the global terrorism, available at ssrn.com) accessed on 15/10/09

individuals with landmines, booby traps etc. based on the RFID tags.

The dependence on information infrastructure gives an unprecedented opportunity for terrorists to aim at targets that would otherwise be extremely difficult to handle, and certainly impossible to be remotely disturbed, like air or road traffic control systems or energy distribution networks. Additionally, a successful attack resulting in enough damage to generate fear is certain to gain extended media coverage, which is a major priority for terrorist actions as it promotes public intimidation. Even though most hacking attacks are kept secret from the public to avoid spread of panic and loss of confidence on the compromised systems, a successful cyber-terrorist attack could not be easily kept away from publicity. Finally, information technology can work as a force multiplier because it allows attacking even the most crucial systems, for example defense and military networks that are certainly very attractive targets for terrorists but were almost impossible to influence before there are also drawbacks for terrorists in exploiting information infrastructure. Even though vulnerable, systems are usually complex. This means that it might be difficult to control an attack and achieve a desirable level of damage or harm. Unless people are injured, there is less emotional appeal and a terrorist attack is less successful. Apart from that, it is probable that terrorists could be disinclined to try new methods and use new tools, unless they consider their old ones inadequate.

Vital systems may depend on information technology, but there is still enough human control to prevent malfunction and cope with emergent and unexpected incidents[25] . Moving towards the second level of assessment, that is evaluating the actual use of information technology as a helpful tool by terrorists, one can draw an initial assumption. We have already seen that terrorist groups are indeed using information technology, but the situation is not much different than with the use of other forms of technology.

As for the general use of information technology by terrorists, it has already been said that terrorists do use information technology as a communications medium, as a means to recruit supporters, collect information, disseminate propaganda and raise funds to support their activity. Furthermore, we still do not know the level of their ability to use information technology. It is highly probable that even if a successful attack to a vital system not aiming to cause great damage but only to warn for future actions, as for example a military defense system, had already happened, it would preferably have been kept secret so as to avoid embarrassment and loss of trust As for pure cyber-terrorist attacks, up to present there have been few, if any, computer network attacks that meet the criteria for cyber-Terrorism /digitalized terrorism. Most of the attacks that can be attributed to terrorist groups were launched merely to annoy or intimidate their targets, no great damages have occurred and no lives have been lost. In 1998, ethnic Tamil guerrillas swamped Sri-Lankan embassies with email bombing. This incident, although characterized by US intelligence authorities as the first cyberterrorist attack, did not result in any big damage. Since then, such techniques have been used during the Kosovo conflict in 1999, and they are a usual incident between parties in many conflicts around the world, such as Israel and Palestine, China and Taiwan, India and Pakistan[26] .

These incidents, however, although usually perpetrated by small groups that could be characterized as terrorist, are more a phenomenon of cyber-war than pure cyber-terrorist attacks. As per the report of the National Commission on Terrorism [27] the changing threat of international terrorism, concluded that although the terrorist's toolbox has changed with the advent of the information age, the objectives of the world's terrorist organisations remain the same. The report stated those terrorists are adopting information technology as an indispensable command-and-control tool, but there is still no indication of whether information infrastructure will constitute their new target[28] It is difficult to assess potential harm because we do not know how vital systems would react and we cannot foresee all possible forms of attack. Whatever the measures taken, a risk still remains.

Terrorists will always be a little ahead of counter-terrorism technology curve, because they spot Vulnerabilities and launch their attacks, always well organised and planned, against them[29]. Terrorism has traditionally provoked such intense concerns that there has always been a temptation to be careless in choosing the weapons to fight it. The fear that it inflicts lies in undermining individual rights and liberties, that otherwise wouldn't stand a chance of being accepted by the public[30]. Therefore it is important to assess the real threat posed by terrorist groups using information technology; keeping in mind that digitalized terrorism is not a term encompassing any use of information technology by terrorists but a real threat to humanity.

Conclusion

Certainly computer and Internet are becoming an essential part of our daily life. They are being used by individuals and societies to make their life easier. Tremendous role of computers stimulated criminals and terrorists to make it their preferred tool for attacking their targets. As per analysis it seems that they prefer using the cyber attack methods because it is cheaper than

[25]Dorothy E. Denning, *Activism, Hacktivism, and Cyberterrorism: The Internet as a tool for influencing foreign policy*, Internet and International Systems: Information Technology and American Foreign Policy Decision making Workshop, at <http://www.nautilus.org/info-DIGITALIZED TERRORISM: A CALL FOR GOVERNMENTAL ACTION? Available at http://www.bileta.ac.uk/01papers/mitliaga.html at p.15. accessed on 23/10/09

[26]Tania Hershman, *Israel's Seminar on Cyberwar*, 10/01/2001 Info Sec News at <http://www.securityfocus.com/frames/?content=/templates/archive.pike%3Flist% 3D12%26mid%3D155550>. accessed on 23/10/09

[27]Report of the National Commission on Terrorism, *Countering the Changing Threat of International Terrorism*, available at <http://www.fas.org/irp/threat/commission.html>.

[28] Dan Verton, *Terrorists use new tools, old tactics*, 26/06/2000 Federal Computer Week, available at <http://www.securityfocus.com/templates/headline.html?id=7408>. accessed on 23/10/09

[29]M. Devost, B.K. Houghton and Neal A. Pollard, *Information Terrorism: Can you trust your toaster?*, available at <http://www.terrorism.com/documents/suntzu.pdf> accessed on 23/10/09

[30]Testimony of David B. Kopel, *Hearings on Wiretapping and other Terrorism Proposals*, Cato Institute - Committee on the Judiciary US Senate, 24 May 1995, at<http://www.cato.org/testimony/ct5-24-5.html>.

traditional method of crime and the chief reason is the action is very difficult to be traced so they can hide their personalities and location. Information technology is boundaryless so there are no physical barriers or check points to cross. They can do their act remotely from anywhere in the world. Unfortunately at a time they can target number of innocent people without moving a bit. The role of Interpol, which is working with 178 member countries to fight against the digitalized terrorism, is good. For this Interpol is helping member countries by training the personal of all the member countries. Another efforts at International level in the name of International treaty is The council of Europe convention on Cyber Crime, which is the result of 4 year work by experts from the 45 member and non-member countries including Japan, USA, and Canada.

In order to combat this type of terrorism lots of efforts should be done at the personal level, country level and at global level. The fact that information technology is widely available and is indeed being used by terrorists initially suggests that there is a call for special governmental action, aiming to eliminate the risks stemming from terrorists taking full advantage of it and enhancing their activity. Terrorism has traditionally provoked such intense concerns that there has always been a temptation to be careless in choosing the weapons to fight it.

In India an enactment of Information Technology Act, 2000 came and to give effect to its provisions appropriate amendments have been made in the I.P.C, 1860, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934. These amendment are not enough to fight the new digitalized terrorism therefore a new "chapter" dealing with "Digitalized terrorism ," can be added to the already existing criminal statues to make them compatible with modern forms of terrorisms. Similarly, a new "chapter" dealing with digitalized terrorism, can be incorporated in the Information Technology Act, 2000 by way of its amendment to bring harmonization among various laws.

The menace of digitalized terrorism is not the sole responsibility of State and its instrumentalities. The visionary citizen is the need of hour, in fact; they are the most important and effective cyber-terrorism/ digitalized terrorism, eradication and elimination mechanism. Therefore it is recommended to encourage them to come forward for the support of fighting against cyber-terrorism/ digitalized terrorism, for this the government must provide them the security in terms of person and property. The courts should be empowered to maintain their anonymity if they provide any information and evidence to fight against digitalized terrorism.

The judiciary can play its role by adopting a stringent approach towards the menace of digitalized terrorism but the jurisdictional issue must, however, first tackle because before invoking its judicial powers the courts are required to satisfy themselves that they possess the requisite jurisdiction to deal with the situation. Although by virtue of section 1(2) read with section 75 of the Information Technology Act, 2000 the courts in India have "jurisdiction" to deal with digitalized terrorism, but the missing knowledge and trained staff it is worthless. Till the uniformity is missing implementing machinery should be empowered to fight the evil of cyber-terrorism/ digitalized terrorism. Further since the Internet "is a cooperative venture not owned by a single entity or government, there are no centralized rules or laws governing its use? The absence of geographical boundaries may give rise to a situation where the act legal in one country where it is done may violate the laws of another country. This process further made complicated due to the absence of a uniform and harmonized law governing the jurisdictional aspects of disputes arising by the use of Internet. Therefore global cyber law is the needed in the era of globalization.

It is important to assess the real threat posed by terrorist groups using information technology; keeping in mind that cyber-terrorism/ digitalized terrorism is not a term encompassing any use of information technology by terrorists.