COUNTERSTRIKE MECHANISM AGAINST NEO-TERRORISM:

Preventions against Cyber Terrorism

Vatsala Sharma,
Under Graduate, B.A. L.L.B (Hons)
Shruti Katiyar
Assistant Professor
Uttaranchal University, Law College Dehradun
Dehradun, India

Abstract

Change is inevitable and the disadvantages that advancement in technology poses cannot be avoided. The fact is that the criminals have changed their methods and have started relying on the information technology, and in order to deal with them the society, the legislative, and the judiciary, the private corporations and public organizations will also have to change their defences to combat cyber terrorism and warfare. Further cyber and techno-experts must not only be assiduous in the field of cyber space and information technology, but must also be provided with necessary technical hardwares and softwares so that they can efficiently fight the cyber criminals. Hence, appropriate facilities must be established in different parts of the country so that crime in the virtual world can be controlled.[1] Another aspect which needs to be brought into limelight is that a culture of continuous cyber education and learning needs to be inculcated amongst the law adjudicating and law enforcing authorities, because the sphere of information technology is quite dynamic as the knowledge of present day becomes obsolete in a very short time. Lastly, the preamble of the Information Technology Act, 2000 states that the Act was passed with the objective to give legal recognition for transactions carried out by means of electronic data exchange and other means of e-commerce, further the Act strived to make amendments to the Indian Penal Code 1860, Indian Evidence Act 1872, The Bankers Books of Evidence Act 1891, and the Reserve Bank of India Act, 1934 for enhancing legal recognition and regulation of the commercial activities. Though the objective of the Act is not to diminish criminal activity, but this Act has defined certain offences and penalties to overpower such omissions, which is understood to come within the circumference of cyber-crimes. From this, it can be concluded that the laws cannot afford to be static, they have to be changed with the changing times and viz. cyber space. This is all the more required, that many applications of the technology can be used for the advantage of the mankind, similarly it is equally true that such applications can also be used for the disadvantage of the mankind as has been demonstrated by the Spy-cam case. The moral here is that the law should be made dynamic so that it can easily adjust to the needs of the times and with the technological developments.

INTRODUCTION

In the era of Information Technology, the rapid development of computers, telecommunications and other technologies has led to the evolution of new forms of cross-national crimes known as "cyber-crimes". Cyber crimes are "any crime which is committed with the help of computer and telecommunication technology", with the purpose of disrupting the functioning of computer or computer systems. To comprehend cyber-terrorism as a significantly new phenomenon, with profoundly new repercussions, it is necessary to recognize it as a constituent aspect of the wider political, social and economic reconstruction currently affecting countries internationally. Free transmission of uncensored information on electronic networks and web-sites is as essential to insurgents and extremists groups as it is to dissidents proclaiming their human rights. Just as crimes have changed with the growth of cyber space so have the categories of criminals, who engage in such crimes, changed.

With the use of computer system and internet day by day, it has become easy to access any information easily within a few minutes by using internet. Certain precautionary measures should be taken by citizens while using the internet

[1] Cyber cell of the law enforcement agencies have started operating in metropolitan cities like Pune, Mumbai, Hyderabad, Chennai, Bangalore etc

which will assist in challenging this major threat of Cyber Terrorism. It is observed, by majority of the organisations that the benefits of cyber revolution have reached in each and every nation of the world. Neither the most of the nations of the world have got separate laws, mutual agreements and multilateral treaties between them to deal with the problem of cyber terrorism and cyber-crimes, though there are some international agreements, conventions, declarations, protocols or resolutions to manage the cross border cyber terrorism, but majority of them are not ratified by the states in international community. The absence of ratification of major world communities has made countries vulnerable to the threats of cyber warfare and terrorism. Therefore, there is no opposition to the fact that an international agreement on the ways and means of dealing with cyber terrorism is urgently required to address the menace in a hostile manner. The foul repercussions associated with the use of malware are not peculiar to any particular country as the consequences are global in nature. The communities all over the world are facing this problem and are trying their level best to prevent this problem. The menace, however, cannot be effectively dealt without support of popular public and judiciary.

The legislature cannot enact a law against the general public opinion of the nation at large. Thus, first a public consensus has to be obtained not only at the national level but at the international level as well. The people all over the world are not opposing the enactment of statutes preventing the use of malware, but they are conscious about their legitimate rights. Thus, the law to be implemented must take care of public interest on a priority basis. This can be done if a suitable technology is supported by an appropriate legislation, which imperatively can take care of the situations created by the computers transmitting the malware. Thus, the self-help measures promulgated by the legislature should not be disproportionate to the threat received by the malware. Further, due to the use of many self-help measures, the property and rights of the general public should not be affected. It would be reasonable to demand that such self-help defences should not themselves commit any illegal act or omission. Thus, a self-help measure should not be such which may destroy or mutilate the data or secret information stored in the computer of the person to whom the malware is transmitted. Thus, a differentiating line between self-defences and taking law in one's own hand must be drawn.

AN ANALYSIS OF THE PROBLEM OF CYBER TERRORISM

In the analysis, it must not be overlooked that self-help measures are "watchdogs and not bloodhounds"', and their support should be limited to legitimate and proportionate defensive actions only. In India, fortunately, we have a healthy legal foundation for dealing with malware and the public has no opposition in supporting the defensive measures to combat cyber terrorism. If still there exist any discrepancy, then it will be appropriate to mention that only a computer can take quick actions to take care of the predicament of malware and the traditional methods of the executive and judiciary would be helpless in that regard. The problems of lack of harmony, lack of uniform extradition laws between various countries of the world, etc. can be simplified by enacting legislations that are provide defences against cyber terrorism and are also prompt and not intricate.

The menace of cyber terrorism is a dynamic in nature and requires a law which is as dynamic as the problem itself. The major issue within the field of law is that we don’t find a law and enact it till the time comes when the waters rise and a crime reaches its summit poking holes through the well-established lawful society. At that point of time, it becomes quite intricate to deal with the problem, if not completely impossible. The main obstacle in enacting legislation against cyber terrorism or any crime against the information technology is that the measures in form of legislations are not enough to deal with the menace created by such crimes, but what needs to be understood here is that having something is always better than having nothing in hand. The solution to any legal problem is enacting and implementing progressive, dynamic laws which serves as a stich in time.

Hence, the moral of the story lies in the fact that though the world is cherishing the information technology and its use in the present times, but it cannot be overlooked that the cherished advantages of the information technology and cyber space, are rendering quite discomforting threats on the privacy of nations which in turn paint the canvas of the cyber space in quite dark and foul shades.

MECHANISMS OF CYBER TERRORISM

There are three methods of launching and inflicting any Cyber Attack which are basically launched upon only computer systems, by way of viruses and malware, hence sometimes the word “cyber terrorism” is said synonymous to “computer terrorism”. The three prominent ways of launching cyber terrorist’s attacks are-

1. Physical Attack- whereby the computers are damaged, mutilated, vandalised by way of bombings or firing them up. These are the conventional methods of disrupting computer networks, used previously by the terrorists.

2. Syntactic Attack- under this method of attack, the computer systems are made to delay or made unpredictable by introduction of viruses, malware or Trojans. Viruses, malware and Trojans are the main weapons by which such attacks are launched.

3. Semantic Attack- in such kind of attacks, the information of the computer users is used and manipulated in such a way that it demolishes their confidence. In an article published in “Where are your cyber-attacks coming from?” in “Verizon’s” “DBIR 2015”, compiled by the research community “Tripwire”, it was said, “there are five most common attack patterns of 2014 of a cyber attack, which were-

   a. Web Application- those cyber-attacks that are committed as organised crimes.

   b. Privilege Misuse- those cyber-attacks that happen for financial gains.

   c. Cyber Espionage- those attacks that affect the manufacturing, professionals and public authorities.

   d. Crimeware

   e. Point of Sale

SUGGESTIONS TO PREVENT FROM NEO-TERRORISM

There are quite a few suggestions which are required to be paid heed for the protection of cyber space from cyber terrorism. The prominent ones amongst them being of the kind, that the judges and the judiciary of the world need to be more technologically sound- accepting e-documents to be of evidentiary value, giving electronic justice for speedy remedies and trails, plus formulating Electronic Code of Criminal Procedure in the courts for efficient trials, and the like.

It has been observed that generally, the age of hackers lie between those of teenagers and adolescents, hence they must be made aware about the ill effects of hacking and the acts of the same kind. It is because of their unawareness about the consequences of their actions. The hackers are also not aware about the deterrent provisions of cyber laws pertaining in India and International level. Thus, in the education system, cyber ethics should be incorporated in course syllabi. The skills of children assiduous in the task of hacking should be used for constructive purposes. Though, it is not expected from a judge to possess technologically sound knowledge to deal with cyber-crimes, but for this purpose they sure can seek expert opinions from people who are skilled in this field. Similarly, when a person commits cyber terrorism outside the territory of India, damaging software within the Indian territory, then the procedure in the laws laid down for the trail and conviction of these offenders are quite intricate, hence, another suggestion that lies here is that laws with regard to such offenders should be made comprehensible and easy.

Apart from this, the basic need in context of prevention of Cyber Terrorism, is to spread awareness regarding the disadvantages of hacking, the penal sanctions against them and the consequences that these practices have, plus-

1. A need of a comprehensive law with regard to cyber terrorism still is paramount that defines cyber terrorism and lays down as to what are the penalties and punishments on indulgence in it.

2. Government agencies should be able to operate their own systems with high security measures, confidential fibre and the like to prevent any mis-happening from cyber terrorism.

3. Updating the anti-viruses and anti-malware software and bringing them into usage is another necessary step to be taken into consideration.

4. Enhancing IT education for the youth, the bureaucrats, the administrators and as well as for common people is necessary and indispensible.

5. Connection of network systems with one another so that any information which is being transmitted by any mobile phones, laptops, computers, etc, in the cyber space can be known by the government security officials.

6. Law enforcement personnel must be trained to handle cyber crimes and to find solution and prevention of the same.

7. Private sectors of the country should focus upon spreading awareness with regard to ill effects of cyber terrorism and sponsor in such programmes as well.

8. Adopting ICT standards and regulations for high quality security services that are required in computer systems.

PREVENTIVE MECHANISM

Apart from these some precautionary methods used for prevention of cyber terrorism in the IT field are-

1. Firewalls- these are programs that protect users from unauthorised attacks from any source via messages on networks.

2. Changing of passwords- a user must always keep changing his passwords, for the sake of it not being known to any other person who would then misuse the account of user.

3. Checking for viruses frequently- just like frequent medical check-ups are required to be done on a human body, similarly, computer systems should also be frequently checked with regard to presence of any viruses and malware. It provides a precautionary and protective measure against cyber terrorism.

4. Providing filters on mailing accounts- E-mail filters must be provided to every user of social sites to prevent the influx of suspicious mails containing malware and viruses.

CONCLUSION

Use of such methods will definitely ensure decrease in the rate of cyber terrorism acts in the country and at international levels. Just as a stich in time saves nine, the need for enactment of policies that have been enshrined as guidelines under International Conventions, is supreme at this point of time. The menace of cyber terrorism created needs to be resolved so as to prevent occurrence of the so-predicted “IIIrd War” or the “Cyber War” amongst the international communities. Myriad measures have been adopted yet they need to be promulgated with a rod of deterrence in hand so as to prevent or minimise the happenings of such attacks. As it is said, a proverb is not a proverb till you have faced it, similarly the problem of cyber terrorism must not be taken lightly so as to later “cry over spilt milk.”

Hence, it is better to enact laws and policies within time being at hand so as to prevent any future epidemic of the small trouble existing now. This was thus, the need to undertake this research so as to bring into limelight the problems caused by cyber terrorism, the laws and conventions in existence against cyber terrorism, grey areas and lacunae in the laws with regard to cyber terrorism and the preventive measures to be adopted against the same, coming to the point of taking the problem of cyber terrorism as an opportunity create a new solution for it which will hence save the world from its clutches, which brings us to the what was said by Winston Churchill,

“The pessimist sees difficulty in every opportunity and the optimist sees opportunity in every difficulty”[2]

[2] Sir Winston Leonard Spencer Churchil KG OM CH TD FRS PC PC (Can) (30th November, 1874- 24th January, 1965)