Countering cyber terrorism in india criminology essay

1. Cyber terrorism is planned use of disruptive activities, or the threat of the same, against computers /networks, with the purpose of causing harm or further social, religious, political or comparable objectives, or to intimidate anyone in furtherance of such objectives. With the “ Love Bug” virus costing nearly $10 billion, it is difficult to comprehend the financial implication of a more serious & comprehensive attack. Each & every day, corporations all over the world spend crores combating threats of cyber attacks & cyber terrorism. With the increased occurrence of attacks, the cost will drastically increase in the coming years.

2. The Internet being disrupted for just one day could disturb nearly $6. 5 billion worth of transactions. More than just the eCommerce transactions stream over the Internet. Email, voice connections, banking machines, credit card authorizations for stores, and the list is endless. Info is the life blood of business, regulatory oversight & even social status. The importance of the info & the ability to access it, transfer it & act upon it has increased to a point that it is unimaginable for all but the smallest of businesses to function without computers or networks. As the value of computing infrastructure increases so to does the value of its disruption. Financial implications are one thing, but the psychosomatic impact could be even more damaging.

3. Cyberterrorism is the next big terror campaign that India is likely to face, as per the Intelligence Bureau[35]. Already, the agency has given numerous warnings on cyber attacks. Initial signs of tech-savvy terrorists came to prominance during the serial blasts that shocked the country a year ago. However the question, is how geared up is the country to face the threat?

4. Reports indicate that for a radical organisation, the easiest way to initiate an attack on India would be via the cyber route. It is high investment, but saves the trouble of manpower on the field, & the impact such an attack could be is immense. The terrorist organisations could begin an Internet war by hacking into official websites and sending out viruses to subvert the nation. The cyber assaults could include cyber vandalism, damage to (ESCOMs) essential commodity-related sites and phishing.

5. The cyber war on India is expected to be fought in three stages[36]. First the en could bring down the control systems of defence installations/infrastructures, Parliament, railways & airports. Next, they could attack financial services such as banks & stock markets. Lastly, ESCOMs & other utilities services could be taken over. This is a dangerous scenario & it will create a lot of panic, & if they succeed, it would cause a lot of destruction, since it could take days before the services would actually recover.

6. Experts also assess that although the Pak-based terrorists could prove lethal, the worst attack are likely to come from China through use of the Distributed Denial of Services attacks. In a DDOS attack, bandwidth of a targeted system is swarmed. They attack the other systems by multiplying and creating botnets. Though India has had its share of these attacks, but as of yet they have not been on a large scale. The sector targeted the most in the attacks is the telecom sector, but it has managed to survive, thanks to a strong infrastructure. However, the companies have to constantly improve, to be one up on the enemy.

Fig 1 – Defacement of Indian Websites[37]

Defending against the New Terrorism[38]

7. Traditional Method. Defending against terrorism where a computer or the Internet plays an important part in the terrorism matrix is very similar to defending against terrorism that does not. The regular practices are still effective, except that the scope of certain elements is expanded. These techniques are often presented, and can be to be updated to include their ‘ virtual’ counterparts. Traditional counterterrorist techniques[39]are :-

(a) Deterrence. Governments can use their coercive capacity to make terrorism too costly for those who seek to use it. They can do this by military strikes against terrorist bases, assassinations of key leaders, collective punishment, or other methods. There are several drawbacks to this approach, it can lead to unacceptable human rights violations. In addition, groups may not come to government attention until movements are so well developed that efforts to contain them through deterrent methods are insufficient.

(b) Criminal Justice. Governments can treat terrorism primarily as a crime and therefore pursue the extradition, prosecution, and incarceration of suspects. One drawback to this approach is that the prosecution of terrorists in a court of law can compromise government efforts to gather intelligence on terrorist organisations. In addition, criminal justice efforts are deployed mostly after terrorists have struck, meaning that significant damage and loss of life may have already occurred.

(c) Enhanced Defence. Governments can make targets harder to attack, and they can use intelligence capabilities to gain advance knowledge of when attacks may take place. As targets are hardened, however, some terrorist groups may shift their sights to softer targets. An example is the targeting of US embassies in Kenya and Tanzania in August 1998 by truck bombs. Targets in Africa were chosen because of their relatively lax security compared with other targets.

8. Thwarting Cyber Terrorism.

(a) Securing info infrastructures will require substantial efforts. Close collaboration between govt and the private sector is important. The govt must introduce tougher penalties for such crimes & increased funding for law enforcement efforts to fight it. This must be achieved with a high degree of cooperation globally.

(b) Computer & information security, data security, & privacy are all emergent problems. No single technology/ product will eliminate the threats & risk. A global strategy & policy for combating this kind of terrorism is the need now. In 1998, a 12-year-old hacker in US broke into the computer system that controlled the floodgates of the Theodore Roosevelt Dam in Arizona, according to a Washington Post report[40]. If the gates had been opened, the article added, walls of water could have flooded the cities of Tempe and Mesa, whose populations total nearly 1 million. The incident serves as a metaphor for today’s pressing debate over the Internet’s vulnerability to attack.

9. International Efforts Of Combating Cyber Terrorism. Interpol, with 178 member countries, is combating cyber terrorism. They are helping the member countries and training their pers. The Council of Europe Convention(CEC) on Cyber Crime, which is the 1st international treaty for combating computer crime, is the result of four years work by experts from the 45 countries. This treaty has been already enforced after its ratification on 21st of March 2004.

10. Association of South East Asia Nations (ASEAN) has made plans for sharing info on computer security. They plan to form a regional cyber-crime unit. The charter will be :-[41]:

(a) Preventing privacy violations.

(b) Preventing information and data theft.

(c) Preventing distributed denial of services attack (DDOS).

(d) Preventing network damage and destruction.

11. Common Aspects. Currently there are no foolproof ways of protecting a system. Majority of the classified info is stored on machines with no outside connection, to prevent cyber terrorism. Apart from isolation, the most common means of protection is encryption. Encryption, however, does not defend the entire system, an attack intended to disrupt the whole system, such as a virus, is impervious to encryption. Other common preventive measures are also used, but these are more so as protection for individual machines and networks and not very effective means of combating cyber terrorism.

Strategies to Deal with Cyber Terrorism Threats

12. To deal with cyber terrorism, the strategy needs to be put in place. Various steps that can be taken by the parties involved to deal with the threats of cyber terrorism effectively are:-

(a) Pursue and Prosecute the Perpetrators. The parties that have been affected from attacks of the cyber terrorists should be more forceful in pursuing the perpetrators. If there is an increasing number of such attackers that can be brought to justice, it might change the general mindset of the cyber terrorist community.

(b) Develop Security Practices. Organizations should ensure that they develop and deploy a tested set of security practices suited specifically for their own operations. These activities will require a lot of coordinated efforts from all parties in the organization because every department should follow security procedures.

(c) Be Proactive. Organizations and the general public should be more proactive in dealing with cyber terrorism issues by keeping up to date on the latest information related to threats, vulnerabilities and incidents and they should be more committed in improving their information security posture. Organizations should always be looking to improve upon their existing security infrastructure.

(d) Use Security Applications. The use of security applications such as firewalls, Intrusion Detection Systems (IDS), anti-virus software and others should be encouraged and in some cases, mandated to ensure better

protection against cyber terrorism. Organizations should deploy both network and host-based IDS along with other security applications.[42]

(e) Disaster Recovery Plans. The plans should involve two main activities that are repair and restoration.[43]The repair activity should fix the problem in order for the function to operate normally. The restoration plans should be activated with pre-specified arrangements with hardware, software and service vendors, emergency services, public utilities and others.

(f) Increase Security Awareness. Security training programs can assist people to equip themselves with the right skills and knowledge that are needed to protect their computer and networks systems effectively.

(g) Stricter Cyber Laws. The government can assist in controlling cyber terrorism attacks by adopting and revising new cyber laws that will punish the perpetrators more heavily if they are involved in such activities.

13. Countering Transnational Cyber Terrorism. Efficient struggle against transnational computer crime & terrorism is an essential element of assured security not only with a view of fighting against e-terrorism but also real counteraction to such new kinds of organized crime. Despite such uneasy situation in the sphere of defence, there are some opportunities to solve it: [44]

(a) Organization of efficient cooperation with foreign countries, law enforcement agencies, services & also international organizations to fight cyber terrorism & transnational computer crime.

(b) Forming a national unit to fight cyber crimes and an international communication centre to provide aid at responding to transnational computer incidents.

(c) Extending transnational cooperation in the sphere of legal support to fight computer crimes and cyber terrorism.

(d) Accepting laws on e-security according to the existing international standards and EU Cyber Crime Convention. It is necessary to:

(i) Prevent and avert financing of terrorist acts;

(ii) Introduce criminal liability for deliberate provision or collecting funds to commit terrorist acts;

Block funds and other financial assets or money of persons that

commit or attempt to commit terrorist acts;

(iv) Find opportunity to speed up the exchange of operational information with the purpose to prevent acts of terrorism;

(v) Refuse asylum to those supporting, financing and planning terrorist acts;

(vi) Render assistance in view of criminal investigations related to financing or backing of terrorist acts;

(vii) Prevent displacement of terrorists by assistance of frontier control.

Render thorough cooperation in the framework of multilateral and bilateral mechanisms and treaties with the purpose to prevent terrorist acts;

(ix) Take part in the corresponding international conventions and protocols to fight international terrorism.

Law & Cyber Terrorism

14. Cyber terrorism is a disastrous phenomenon that has not yet attracted the attention of the Indian Government. The law in this regard is not adequate and the predicament of cyber terrorism can be tackled appropriately either by making a separate regulations in this regard or by making appropriate amendments in the already existing Info Technology Act, 2000. There is no law, which is exclusively dealing with prevention of malware through some aggressive defence. Thus, the equivalent provisions have to be applied in very a purposive manner. The defence against malware attack can be claimed under the following categories:-

(a) Protection under the Constitution of India[45]. The protection available in the Constitution of any country is the safest one since it is the highest document and all other laws obtain their power and validity from it.

(b) Protection Under Other Statutes[46]. The protection existing under the Constitution is strengthened by various statutory enactments. These can be classified as :-

(i) Protection under the Indian Penal Code (I. P. C), 1860.

(ii) Protection under the Information Technology Act (ITA), 2000.

15. What India Needs To Do

(a) In India, a reality check with the cyber crime wings portrays a poor picture. When cyber crime cells were set up in the country most cases pertained to sleaze mails. Now the complaints have become more

sophisticated and at an average, four complaints of phishing mails that are there everyday. The detection rate is not something that one can be proud with only one out of four cases solved and a miserable conviction rate. The cyber ceels need to keep updating and deploy new tactics[47].

(b) A combined effort is needed to counter the cyber threat & cyber crime police stations need to be revamped[48].

(c) The Ministry of Finance too has upgraded its infrastructure to prevent cyber strikes. They have introduced a two token system, which mandates that a person carry with him a normal password and also a token that generates pin codes in real time. In key areas such as defence sectors, the use of a personal laptop has been banned.

16. Legal Aspects.

(a) India cannot solve the problem on its own. It will need the help of other countries. However, India is not a signatory to the 45-nation international convention on cyber crimes. Moreover, India still awaits a legal framework on cyber attacks[49].

(b) The description of " cyber terrorism" cannot be made comprehensive as the nature of offence is such that it must be inclusive in nature. The character of " cyberspace" is such that new technologies are invented on a regular basis; hence it is not prudent to put the description in a straightjacket method or pigeons hole. In fact, the effort of the Courts should be to construe the definition as liberally as feasible so that the menace of cyber terrorism be tackled severely.

(c) The law dealing with cyber terrorism is not sufficient to meet the intentions of these terrorists and requires a renewal in the light of the most recent developments all over the world.

(d) The under mentioned can be safely regarded as cyber terrorism :-

(i) Privacy violation. The law of privacy is a recognition of the individual's right to be left alone and to have his own personal space inviolate. Right to privacy is a element of the right to life and to liberty enshrined in Article 21. With the arrival of info technology the traditional concept of right to privacy has taken new dimensions, which require a different legal outlook. To meet this emerging challenge resort to Information Technology Act, 2000 can be taken.

(ii) Secret Information Appropriation and Data Theft[50]. The information technology can be used to appropriate valuable Government secrets and information of private individuals, government and its agencies. Computer networks owned by the Government may contain important information concerning defence and other secrets, which Government may not wish to share otherwise. The same can be under attack by the terrorists to facilitate their activities, to include destruction of property. It must be noted that the meaning of property is not restricted to moveables or immoveables alone. Thus, if a person without consent of the owner or any other individual who is incharge of a computer, computer system, computer network accesses or secures access to such a computer system, damages, causes to be damaged any computer, computer system, computer network, data, or any such other programmes in the computer system, he shall be liable to legal action.

(iii) Demolition of e-governance base. The aim of all cyber terrorist actions is to collapse a sound communication system, including an e-governance base. Thus, by a amalgamation of virus attacks and hacking techniques, e-governance base of a government can be damaged. This would be more harmful and devastating as compared to other tangible damages, caused by the traditional terrorist activities. Likewise, the terrorists to the loss of the nation at large can unlawfully obtain information protected from public scrutiny in the interest of protection of the nation. Thus, a robust e-governance base with the most modern security methods and systems is required.

(iv) Distributed denial of services attack: Cyber terrorists may also use distributed denial of services (DDOS) to overload the Govt and its agencies electronic bases. This is made feasible by first infecting many insecure computers by way of virus attack and then run. These infected computers made to send info or demand in such a large quantity that the servers of the victim collapse. Due to this unnecessary Internet traffic, rightful traffic is prohibited from reaching the Govt or its agencies computers. This results in immense financial and strategic loss to the govt and its agencies. The law in this regard is very clear and individuals indulging in such activities can be prosecuted.

(v) Network Damage and Disruptions. The key aim of cyber terrorist activities is to effect networks damage and their disruptions. This action may divert the security agencies thus giving the terrorists extra time and make their task comparatively easier. This procedure may involve a combination of

computer tampering, virus attacks, hacking. The laws in this regard provide that indls indulging in such acts can be prosecuted.

The Road Ahead

17. The threat of cyber terrorism can be effectively cramped, if not completely eliminated, if the sovereign organs of the Constitution work together and in harmony with each other. Further, an alert citizenry can supplement the assurance of removal of cyber terrorism.

(a) Legislative commitment[51]. The legislature can provide its support to the objective of removal of cyber terrorism by enacting appropriate statutes pertaining to cyber terrorism. A new section dealing with " Cyber terrorism" be added to the previously existing criminal statues to make them attuned with modern forms of terrorisms. Similarly, a section dealing with cyber terrorism be incorporated in Info Technology Act, 2000. The repealment of POTA and its replacement with a new ordinance was an opportunity for the legislature to make the terrorist law effective to deal with cyber terrorism.

(b) Executives concern. The Central Govt and the State Govts can play their role effectively by making rules & regulations dealing with cyber terrorism & its facets from time to time. The Central Govt, by notification in the Official Gazette and in Electronic Gazette, can make rules to carry out the provisions of Information Technology Act. Similarly, the State Govt can, by notification in Official Gazette, makes rules to carry out provisions of the Act. Further, the govt can also block web sites that propagate cyber terrorism. The Indian Computer Emergency Response Team (CERT-In)[52]has been nominated as the sole authority for issuing of directives in the context of blocking a web

site. CERT-In instructs the Department of Telecommunications to block the web sites after verifying the authenticity of complaint and satisfying that the action of blocking of website is absolutely essential.

(c)Judicial response[53]. The judiciary can participate by adopting a stern approach towards the danger of cyber terrorism. But it must first tackle the jurisdiction problem because prior to invoking its judicial powers the courts need to satisfy themselves that they have the requisite jurisdictionto deal with the situation at hand. Since the Internet " is a coop venture which is not owned by a single entity or govt, there are no centralised rules/ laws governing its use. The nonexistence of geographical boundaries may result in a situation where the act legal a country where it is done may violate laws of another country.

(d) Vigilant citizenry: The threat of cyber terrorism is not the sole liability of State. The citizens are equally under a solemn responsibility to fight against the cyber terrorism. As a matter of fact , they are the most significant and valuable cyber terrorism eradication and elimination mechanism. The requirement is to encourage them to come forth for the support of combatting cyber terrorism. The govt can give suitable incentives in the form of monetary awards. However, their anonymity and security must be ensured before seeking their assistance.[54].

Protecting Critical infrastructures

18. There is a need for clear laws and standards which require operators of large networks of Internet-connected computers to exercise appropriate due

diligence in their upkeep and security. To this end, there is an urgent need for definition of a minimum standard of security for computer networks.

19. The above is not exactly a novel concept. International standards have been developed in other areas where safety and security are a concern. Consider the airline industry. There are international guidelines for airport safety; in cases where these standards are not met, consequences range from warnings to prohibited travel.

20. Infrastructures once determined critical, need to be protected. There is a need to look at them from the threats' point of view. The threat could be a to view the vulnerabilities from the threat's perspective, in the form of " Red Teaming". Red teaming is " a technique that involves viewing a potential target from the perspective of an attacker to identify its hidden vulnerabilities, and to anticipate possible modes of attack.[55]" Red teaming deepens understanding of options available to adaptive adversaries and provides groups an insight into their vulnerabilities. The result of a good red teaming session will provide a basis for plans to mitigate risks to critical infrastructures.