A STUDY ON CYBER TERRORISM PROMINENT CASE LAWS AND WAYS TO COMBAT IT

R. Dinesh

[1]4th year BA.LLB HONS department of Law Saveetha School of Law, Saveetha University, Saveetha institute of medical and Technical Science Chennai -600077, India.

Abstract: ***In this research paper we have discussed about the phenomenon of Cyber terrorism and its growing impact in the current scenario. We have reviewed the laws and acts in various countries like US, UK, Canada, Australia and in India. We have also tried to review the Cyber terrorism from the aspect of the Indian IT Act 2000. We have carried out a comparative review of the various laws made by these individual countries to deal with the Cyber Terrorism. In the end we have concluded that the existing laws in various countries are not efficient to restrain the cyber-crimes and, thus urging a need for implementing modifications through which these activities can be prevented. There is a need of international cooperation of nations to crack down the efficiency on the cyber-crime.***

Key words: *Cyber terrorism, cyber-crimes, laws, countries, Prevention, National Security.*

OBJECTIVES:

- To study about cyber terrorism and related case laws in India.
- To known about the impact of cyber terrorism in India.
- To know difference between Indian law and U.S.A law.

HYPOTHESIS:

There is no significant Indian legislation on cyber terrorism pass it stand today is not sufficient to control cyber terrorism.

There is significant legislation in india on cyber terrorism pass it stand today is sufficient to control cyber terrorism.

RESEARCH METHODOLOGY:

The In this paper the research has opted for doctorial research methodology and the sources act collected mainly through secondary data.

LIMITATION:

The research is unable to trace the primary sources needed to write about the topic as the topic demands research in the archives which is not available to the research as admission to the government archives is not allowed to undergraduate students.

INTRODUCTION:

The capability to conduct basic hacks against individual systems using tools created by someone else. The organization possesses little target analysis, command and control, or learning cyber terrorism is the use of the Internet to conduct violent acts that result in, or threaten, loss of life or significant bodily harm, in order to achieve political gains through intimidation. It is also sometimes considered an act of Internet terrorism where terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet by means of tools such as computer viruses, computer worms, phishing, and other malicious software and hardware methods and programming scripts. [1]

The following three levels of cyber terror capability is defined by Monterey group

Simple-Unstructured:

- ***Advanced-Structured:*** The capability to conduct more sophisticated attacks against multiple systems or networks and possibly, to modify or create basic hacking tools. The organization possesses an elementary target analysis, command and control, and learning capability.
- ***Complex-Coordinated:*** The capability for a coordinated attack capable of causing mass-disruption against integrated, heterogeneous defenses (including cryptography). Ability to create sophisticated hacking tools. Highly capable target analysis, command and control, and organization learning capability [2]

The aim of this study to analyze cyber terrorism and its various impact of a country's people and property.

[1] Assessing the risks of cyber terrorism, cyber war and other cyber threats ja lewis - 2002 - steptoe.com

[2] The invisible threat of cyber-terrorism d verton, j brownlow - 2003 - dl.acm.org

We can categorize Cyber-crimes in two ways

The Computer as a Target:- using a computer to attack other computers.

Hacking, Virus/Worm attacks, DOS attack etc. can categorize Cyber-crimes in two ways

1. The Computer as a Target:- using a computer to attack other computer.

   e.g. Hacking, Virus/Worm attacks, DOS attack etc.

2. The computer as a weapon:- using a computer to commit real world crimes.

   e.g. Cyber Terrorism, IPR violations, Credit card frauds, EFT frauds, Pornography etc.

Cyber Crime regulated by Cyber Laws or Internet Laws.

Some of the common, but false messages sent by sexualized culture. [3]

What is Cyber Terrorism?

There is often a large amount of confusion as to what cyber terrorism is. More specifically, what cyber-attacks can we actually define as acts of terrorism? The internet has allowed for a vast exchange of information.

Thus has created a cyber space in which both criminals and terrorists can implement attacks/communications. This use of cyberspace results in there no longer being simply a physical threat of terrorism. When we consider what cyber terrorism actually is, we must first understand the motivations behind cyber-attacks.

Cyber-attacks can come in many differing forms, and it is these forms that help us understand whether the attack is of crime or terror. Figure 1 shows the distribution of cyberattacks across cultural, social, economic and political motivations. Gandhi et al. (2011) discusses that often these dimensions of motivations can often cross over and the motivating factors behind cyber-attacks are needed to be carefully considered when we discuss cyber terrorism [4]

Section 66F of the Information Technology Act, 2000:

66-F. Punishment for cyber terrorism. - (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 [5]

Major cases relating to cyber terrorism:

It has been rightly said that: "Just as a modern thief can steal more with a computer than with a bag, tomorrow's terrorist may be able to cause more damage with a computer mouse than with a bullet or a bomb. "

Case 1. The website of the Bhabha Atomic Research Centre (BARC) at Trombay was hacked in 1998. The hacker's gained access to the BARC's computer system and pulled out virtual data7.

Case 2. In 2002, numerous prominent Indian web sites notably that of the Cyber Crime Investigation Cell of Mumbai were defaced. Messages relating to the Kashmir issue were left on the home pages of these web sites8.

Case 3. In the Purulia arms drop case, the main players used the internet extensively for international communication, planning and logistics.[9]

Case 4. In 2007, the two Indian doctors involved in the Glasgow airport attack used Computers for terrorists activities. Cite case laws - Indian 26/11, Afzal guru (Parliament attack case) Us- World tower attack [6]

Areas of Cyber Terrorism:

As discussed many acts of cyber terrorism are often synonymous with acts of cyber-crime. Thus the means by which attacks are implemented by terrorists may also be done by criminals. These can come in many forms, as discussed by GCHQ and Cert-UK (2015), attacks are often either un-targeted or targeted. These can include, though not limited to: Un-targeted Attacks

• Phishing — These attacks typically involve fraudulent emails to convince a target of it's legitimacy of a user or organisation in order to attain private information (E.g, passwords, banking information, identity theft etc.) ("What are phishing scams and how can I avoid them?", 2017)

[3] Computer attack and cyberterrorism: vulnerabilities and policy issues for congress C Wilson - Focus on Terrorism, 2003 - books.google.com

[4] Assessing the risks of cyber terrorism, cyber war and other cyber threats JA Lewis - 2002 - steptoe.com

[5] Assessing the risks of cyber terrorism, cyber war and other cyber threats JA Lewis - 2002 - steptoe.com

[6] Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy DE Denning - … netwars: The future of terror, crime, and militancy, 2001 - books.google.com

Watering Hole — The deployment of a fake webpage to compromise the original, in order to attack visiting users (e.g the downloading of Remote Access Tools) (National Cyber Security Centre, n.d.) • Ransomware — Infecting a system by encrypting files and/or locking the users access to said system. Then requiring a 'ransom' to gain normal access again. ("Protecting your organisation from ransomware", 2016) • Scanning — Testing for vulnerabilities in specific internet networks or systems to deploy attacks on a wider scale to attack at random (GCHQ, Cert-UK, 2015). Targeted Attacks • Spear-Phishing — These attacks are much the same as the' Phishing' mentioned previously, however specifically targeted at an individual or organisation[7]. • Distributed Denial of Service — This is to deploy a mass amount of packet requests, often from a Botnet , to a 1 website or network in order to overload the system and prevent regular access by legitimate users. • Supply chain — attacking an element of an organisation before it arrives (GCHQ, Cert-UK, 2015). • Zero-day — Bespoke exploitation of a system with specific vulnerabilities not yet known to the author (National Cyber Security Centre, 2016). discussed many acts of cyber terrorism are often synonymous with acts of cyber crime. Thus the means by which attacks are implemented by terrorists may also be done by criminals. These can come in many forms, as discussed by GCHQ and Cert-UK (2015), attacks are often either un-targeted or targeted. These can include, though not limited to: Un-targeted Attacks • Phishing — These attacks typically involve fraudulent emails to convince a target of it's legitimacy of a user or organisation in order to attain private information (E.g, passwords, banking information, identity theft etc.) ("What are phishing scams and how can I avoid them?", 2017) [8]• Watering Hole — The deployment of a fake webpage to compromise the original, in order to attack visiting users (e.g the downloading of Remote Access Tools) (National Cyber Security Centre, n.d.) • Ransomware — Infecting a system by encrypting files and/or locking the users access to said system. Then requiring a 'ransom' to gain normal access again. ("Protecting your organisation from ransomware", 2016) • Scanning — Testing for vulnerabilities in specific internet networks or systems to deploy attacks on a wider scale to attack at random (GCHQ, Cert-UK, 2015). Targeted Attacks • Spear-Phishing — These attacks are much the same as the' Phishing' mentioned previously, however specifically targeted at an individual or organisation. • Distributed Denial of Service — This is to deploy a mass amount of packet requests, often from a Botnet , to a 1 website or network in order to overload the system and prevent regular access by legitimate users. • Supply chain — attacking an element of an organisation before it arrives (GCHQ, Cert-UK, 2015). [9]

Measures being pursued:

As cyber terrorism is one the fastest growing threats, not only to individuals, public and private organisations, but to nations as a whole, we must ensure that the correct methods of prevention are being actioned. This involves both gathering preliminary reconnaissance on potential threats whilst managing current threats. The digital infrastructure each of our nations holds is under constant observation for vulnerabilities, thus cyber security professionals must be ready for an imminent threat from this act of terrorism. Drawing from what we have already discussed in this report, in order for us to look into the current and future measures to take, it would be productive to consider the following pertinent questions: 1. What do we foresee terrorists wanting to do in cyberspace? 2. How can we prevent these actions? 3. How can we be proactive against these actions? We've examined in section three some possible answers to question one. This being that terrorists look to utilise cyberspace in order to: 1. Support their motivation, whether that be their religious, social, cultural, political or economical beliefs 2. Attack critical infrastructures and services in society 3. Utilise cyber space to inflict harm to others In addition to this it's also important to state that cyber terrorists may also employ cyberspace not only to cause harm, but also to facilitate their activities, including the likes of encrypted communications, laundering of finances, recruitment and promotion of their activities. [10]

g. Forgery:-

Counterfeit currency notes, postage and revenue stamps, mark sheets etc can be forged using sophisticated computers, printers and scanners.

Also impersonate another person is considered forgery. [11]

h. IPR Violations:-

These include software piracy, copyright infringement, trademarks violations, theft of computer source code, patent violations. etc.

[7] Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy DE Denning - … netwars: The future of terror, crime, and militancy, 2001 - books.google.com

[8] Assessing the risks of cyber terrorism, cyber war and other cyber threats JA Lewis - 2002 - steptoe.com

[9] Computer hacking and cyber terrorism: The real threats in the new millennium? SM Furnell, MJ Warren - Computers & Security, 1999 - Elsevier

[10] Cyberterrorism: Testimony before the special oversight panel on terrorism committee on armed services US House of Representatives DE Denning - Focus on Terrorism, 2000 - books.google.com

[11] Digital crime and digital terrorism RW Taylor, EJ Fritsch, J Liederbach - 2014 - dl.acm.org

Cybersquatting- Domain names are also trademarks and protected by ICANN's domain dispute resolution policy and also under trademark laws.

Cyber Squatters registers domain name identical to popular service provider's domain so as to attract their users and get benefit from it.

Targeted attacks on military installations, power plants, air traffic control, banks, trail traffic control, telecommunication networks are the most likely targets. Others like police, medical, fire and rescue systems etc. [12] Cyberterrorism is an attractive option for modern terrorists for several reasons.

1. It is cheaper than traditional terrorist methods.
2. Cyberterrorism is more anonymous than traditional terrorist methods.
3. The variety and number of targets are enormous.
4. Cyberterrorism can be conducted remotely, a feature that is especially appealing to terrorists.
5. Cyberterrorism has the potential to affect directly a larger number of people.

j. Banking/Credit card Related crimes:- [13]

In the corporate world, Internet hackers are continually looking for opportunities to compromise a company's security in order to gain access to confidential banking and financial information. Use of stolen card information or fake credit/debit cards are common. Bank employee can grab money using programs to deduce small amount of money from all customer accounts and adding it to own account also called as salami. [14]

k. E-commerce/ Investment Frauds:-

Sales and Investment frauds. An offering that uses false or fraudulent claims to solicit investments or loans, or that provides for the purchase, use, or trade of forged or counterfeit securities.

Merchandise or services that were purchased or contracted by individuals online are never delivered.

The fraud attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site.

Investors are enticed to invest in this fraudulent scheme by the promises of abnormally high profits. [15]

Sale of illegal articles:-

This would include trade of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or simply by using email communication. [16]

CONCLUSION:

Hence I concluded that by saying cybercrime is crime that evolved in large manner and it is detail explain what are all the factor involved in the cybercrime. And cyber terrorism. Hope this paper has given an advance knowledge about the cyber terrorism.

REFERENCES:-

1. Book Black ice: The invisible threat of cyber-terrorism D Verton, J Brownlow - 2003 - dl.acm.org
2. Assessing the risks of cyber terrorism, cyber war and other cyber threats JA Lewis - 2002 - steptoe.com
3. Computer attack and cyberterrorism: vulnerabilities and policy issues for congress C Wilson - Focus on Terrorism, 2003 - books.google.com
4. Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games? M Stohl - Crime, law and social change, 2006 - Springer
5. [PDF] academia.edu Computer hacking and cyber terrorism: The real threats in the new millennium? SM Furnell, MJ Warren - Computers & Security, 1999 - Elsevier
6. Against cyberterrorism M Conway - Communications of the ACM, 2011 - dl.acm.org
7. Cyber terrorism: political and economic implications AM Colarik - 2006 - books.google.com
8. Assessing the risks of cyber terrorism, cyber war and other cyber threats JA Lewis - 2002 - steptoe.com
9. Digital crime and digital terrorism RW Taylor, EJ Fritsch, J Liederbach - 2014 - dl.acm.org
10. Managerial guide for handling cyber-terrorism and information warfare L Janczewski, AM Colarik - 2005 - books.google.com
11. Computer hacking and cyber terrorism: The real threats in the new millennium? SM Furnell, MJ Warren - Computers & Security, 1999 - Elsevier

[12] Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games? M Stohl - Crime, law and social change, 2006 - Springer

[13] [PDF] ccdcoe.org Developing an international cooperation on cyber defense and deterrence against cyber terrorism M Dogrul, A Aslan, E Celik - Cyber conflict (ICCC), 2011 3rd …, 2011 - ieeexplore.ieee.org

[14] Cyber-terrorism in a post-stuxnet world M Kenney - Orbis, 2015 - Elsevier

[15] What is cyberterrorism? M Conway - Current History, 2002 - search.proquest.com

[16] Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy DE Denning - … netwars: The future of terror, crime, and militancy, 2001 - books.google.com

12. Computer attack and cyberterrorism: vulnerabilities and policy issues for congress C Wilson - Focus on Terrorism, 2003 - books.google.com
13. Cyber Terrorism: A Study of the Extent of Coverage in Computer Science Textbooks JJ Prichard, LE MacDonald - Journal of Information Technology …, 2004 - learntechlib.org
14. Cyber-terrorism: The shape of future conflict? A Rathmell - The RUSI Journal, 1997 - Taylor & Francis
15. Cyberterrorism: Testimony before the special oversight panel on terrorism committee on armed services US House of Representatives DE Denning - Focus on Terrorism, 2000 - books.google.com
16. Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games? M Stohl - Crime, law and social change, 2006 - Springer
17. [PDF] ccdcoe.org Developing an international cooperation on cyber defense and deterrence against cyber terrorism M Dogrul, A Aslan, E Celik - Cyber conflict (ICCC), 2011 3rd …, 2011 - ieeexplore.ieee.org
18. Cyber-terrorism in a post-stuxnet world M Kenney - Orbis, 2015 - Elsevier
19. Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy DE Denning - … netwars: The future of terror, crime, and militancy, 2001 - books.google.com
20. What is cyberterrorism? M Conway - Current History, 2002 - search.proquest.com