LEGAL LOCK JOURNAL

2583-0384

VOLUME 2 || ISSUE 5

2023

CYBER TERRORISM: INDIA

Avantika Thankam

ABSTRACT

The author through this paper aims to cover the topic of data privacy and how it is important in the cyber world as a matter of fact how it can be misused by terrorists which constitutes cyber terrorism and the measures taken by the government to prevent the breach of data privacy and also the awareness of the public in general towards cyber terrorism

This article broadly focuses on India and what are the measures introduced as of now by the government as well as the initiative taken to reduce the occurrence of these incidents in the future to prevent the incidents from occurring in future

INTRODUCTION

Cyber laws are the law concerned with regulating the computer and the internet as well as the digital circulation of information and software. And cyber law covers aspects related to the transaction which happens also on the activities over the Internet as it keeps a check on them. One of the most important aspects of the cyber world is privacy which is one of the most essential elements for the survival of mankind as well and also privacy ensures a peaceful life of dignity and also makes an important part of Article 21 of the constitution which also states that privacy is an important part and the article now has been interpreted that way. The right to privacy was recognized as a fundamental right in the case of Justice K S Puttaswamy vs Union of India and Ors. Also, because computers and technology are becoming an important part of the way of life they are being used by people in massive numbers and this increase in computer usage by people has been taken advantage of by terrorists by making it their preferred tool to target people.

CONTENT

"*If you think technology can solve your problems, then you don't understand the problem and you don't understand the technology*"[1]. These were the words of Bruce Schneier which means that even though technology has made our life simpler and easier it also has its negative effects.

[1] David Sutton,cyber security,Oreilly.com,19 March 2023 9 am https://www.oreilly.com/library/view/cybersecurity/9781780173405/19_chapter08.xhtml.

As technology is becoming more prominent the issue of data privacy comes into place and the requirement for the protection of data is very crucial. Law and technology are interdependent and through the introduction of various technology it has become difficult to protect information and keep its confidentiality fact that there is a lack of data-related law that should be addressed

No one shall be subjected to arbitrary interference with privacy, family, home, or correspondence nor attacks upon his honor and reputation. Everyone has the right to protection of the law against such interference or attacks[2]. In India, the data of the citizens are the national assets and it has to keep within the boundaries of the nation these assets have to be protected this can be also applicable to the cooperates as well as the NGOs.

The government can interfere with the data when they feel that the disclosure of the concerned information may lead to a compromise in national security, sovereignty, and also with the integrity of India, friendly relations, or public order when there is a violation of the law or fraud. This is section 69 of the IT Act 2000[3]

The parliament has released a Digital Personal Data Protection Bill which took away the word consent as it was said that the organization doesn't have to ask for consent but inform in clear and plain language for what purpose the data is being collected and for which it is being processed as soon as it is reasonably practicable[4]. The fact that companies just won't get down away with the consent part of the bill because even don't read the policy agreements as the companies flash a long lengthy document and wait for the individual to just accept it even when they understand that the individual doesn't understand the contents and also the fact that the bill weakens out the notion of consent even further here some exception to the collection of consent can be understood as reasonable but the introduction of this bill has created a sense of fear in the people.

Cyber Terrorism

It is often defined as an attack which is against the information system, programs, and data different organization view this attack and defines it in different ways

[2]Yash Gupta, privacy rights and data protection, legal service India,19 March 2023 10:30 am https://www.legalserviceindia.com/legal/article-3609-privacy-rights-and-data-protection.html.
[3]Sneha mahawar, data protection laws in India,ipleaders,19 March 2023 11:00 am https://blog.ipleaders.in/data-protection-laws-in-india-2/.
[4]Justin Sherman, Indias new data bill is a mixed bag for privacy,Atlantic council,19 March 2023 12:00 pm. https://www.atlanticcouncil.org/blogs/southasiasource/indias-new-data-bill-is-a-mixed-bag-for-privacy/

The North Atlantic Treaty Organization, known as NATO, *has defined cyberterrorism as a cyber-attack that uses or exploits computer or communication networks to cause "sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal*."[5]

We are at risk. Increasingly, America depends on computers. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb." At the same time, the prototypical term "electronic Pearl Harbor" was coined, linking the threat of a computer attack to an American historical trauma[6]

So, for a cyber-attack to be cyber terrorism it has to be politically motivated it also has to cause physical or other forms of disruption like attacks affecting the sovereignty, unity, or integrity of the country. Cyberterrorism consists of two aspects one is terrorism and the other is the involvement of cyberspace

Cyber-terrorist groups aim to create a lot of chaos, disrupt critical infrastructure, disrupting political activism. They target is also a computer and the means used will also be a computer as well the main target of terrorism is secured networks of government which will have the data related to national security, data of the citizen, and getting the data into the wrong hands can affect the country in a negative way

Terrorists now moved into cyberspace to facilitate their communication and how to advance their agenda even though this activity doesn't constitute cyberterrorism in a strict sense but they are more acquainted with using the technology and many terrorists are using encryption which helps them to conceal files and their communication and also the fact that one of the biggest advantage a person has while committing a cyber-attack is of anonymity

One of the examples would be in 1998 the ethnic Tamil guerrillas swamped the Sri Lankan embassy with 800 emails per day over a period of two weeks and the message they sent stated "We are the black tigers and we're doing this to disrupt your communication". This was one of the first attacks recognized by the authorities had done toward a country's computer system and also in

[5] Robert sheldon, katie hanna, cyberterrorism, tech target ,19 march 2023 12:30 pm. https://www.techtarget.com/searchsecurity/definition/cyberterrorism.
[6] Bogdanoski, Mitko, and Drage Pitreski. "Cyber Terrorism- Global Threat." *International Scientific* 19 march 2023 1:00 pm.

1999 NATO computers were blasted with email bombs and also hit with denial-of-service attacks by hacktivists protesting the NATO bombing

But to what extent these activities can be included in cyberterrorism as whether these activities were politically or socially motivated or whether they were sufficiently harmful or frightening enough is something still debatable but these instances can be taken as examples to understand that cyberspace has been started to get utilized by the terrorist. They can also engage as a way of financial physical operation. The main domains where the terrorists focus are control systems and data as they can either use the internet as a means to steal or leak data for their benefit. As there is a development in technology as well as cyberspace terrorist outlets are using it as a method to expand themselves mainly through social media.

Even though many weaknesses of the computer can be corrected it is impossible to eliminate them all and even if the technology is offering good security, it is possible to configure ways to make it open for attacks. But some scholars believe that cyberterrorism cannot be used for physical mass destruction rather they create a path for mass destruction one such example would be the attack on Chornobyl which was held on the 25th and 26th of April 1986 example where a cyber-attack caused mass destruction. The monitoring system of the nuclear power plant had suffered a blast and the cause of it was the fact that the monitoring system was claimed to be hacked. Also, these terrorists can use the web pages as they design the content on it how to make weapons and it helps them to identify who has engaged with the website the most and this becomes an effective method of recruiting

INDIAN CONTEXT

India is one of the most vulnerable nations when it comes to cyber-attacks and the reason for this is that most activities like telecommunication, business, etc are dependent on technology and also they are not protected by proper measures

Awareness about cyber terrorism in India is really poor. The whole dark web which is the breeding site of a lot of different illegal activities will also fall under the ambit of cyberterrorism.

The prominent incidents which happened are

- In 2010 the website of the central bureau of Investigation was hacked by some Pakistani hackers called the Pakistan hackers army and yet India's approach has been not satisfactory and no system for cyber security was established
- In the summer of 2011 India was hit by a virus attack at Indira Gandhi International Terminal New Delhi where the check-in counters transfer counters and boarding gates became non-operational and which as a result caused the airline to be non-operational as the common use passengers processing system became non-operational. It was after 12 years the system got restored and later the investigation revealed that someone had hacked the main system of CUPPS
- Another example of the same would-be Mumbai terrorist attack also known as the 26/11 Mumbai attacks which was a wakeup call where the Pakistani militants gained access to the location with the help of google earth not only it was used to plan the whole attack but other technical tools were used to plan and plot the attack when they attacked the taj hotel they were able to gain information by accessing the hotel's computer.

Government after the incident of the bomb explosion of 2010 at Varanasi followed by the bomb explosion in 2011 at Zaveri bazar of Mumbai and by the occurrence of these incidents the government adopted measures for a string of cyber security measures by amending the Indian Information technology act of 2000.

The issue of data privacy and cyber terrorism can be connected in the way that if the terrorist gets hold of the information it can target security if they get access to the sensitive information and the fact that citizens trust people with their data and access to the data by another individual or an organization will be a breach of privacy which in turn can cause the individuals to lose faith in the system.

Cyberterrorism can be classified into four main categories[7]

1. Hate propaganda-which is mainly used as a loophole of the right to expression in India
2. Virus attack and hacking-which is the unauthorized access of the computer system and this is more towards the government website through which they steal the data

[7] Jobin Sebastian, P. Sakthivel, CYBER TERRORISM: A POTENTIAL THREAT TO NATIONAL SECURITY IN INDIA,19 march 2023, VOL 7, ISSUE 15, 2020 , Journal of critical review, 2020 https://www.jcreview.com/admin/Uploads/Files/61f2623012d077.55808485.pdf.

3. False propaganda -Terrorist groups try to spread their strategies and policies through social media
4. Undermining of right to privacy-This is more towards women and children like child pornography, cyber morphing

The threat of cyberterrorism is one of the techniques which are being used as they gain access to computers, they disrupt sensitive information which will endanger national security and also the life of people, and the fact that information that is the most sensitive to people are linked through the cyber networks so it's pretty alarming.

Cyberterrorism can occur on specific aspects which includes

- Destroying the databases of air, and military bases
- Causing different attacks on different sites of the country which can cause monetary loss and also a loss in the data
- Affecting how technology functions and due to which the system has caused errors it may lead to the loss of lives

MEASURES INTRODUCED

India has introduced a privacy policy as well as new encryption to take on the growing cyber security challenges like the enactment of the Information Technology (IT) Act 2000 the setting up of the Indian Computer Emergency Response Team, a Framework for enhancing Cyber Security (2013) National Critical Information Infrastructure Protection Centre (NCIIPC) under the IT Act, 2000, National Cyber Security policy (2013) which are some of the measures taken by the government to tackle the problem of cyber security. The government has introduced a national cyber security strategy but is yet to implement the same

Indian computer emergency response team was also introduced of which the primary purpose is to provide alerts immediately which challenge cyber security and would also list out emergency measures that would help to maintain the cyber security of the nation as well.

Different laws have also been enacted for the same which are under the information technology act 2008 and section 66F of this act has enacted legislative enactment which prescribes the punishment for this act: -(A)

- Person threatening the sovereignty and integrity of the nation or striking terror in any section of people
- Attempt to access a computer resource without authorization
- Denial to any person who is authorized for the computer resource

and engages in conduct that has the potential to harm the critical information infrastructure listed in Section 70, damage or disrupt supplies or services that are necessary for the community's survival, or cause or is likely to cause death, bodily harm, damage to, or destruction of property.[8]

(B)-

knowingly or intentionally violates or accesses a computer resource with no consent, surpasses authorized access, and utilizing such conduct obtains access to restricted information, data, or computer databases for national security or international relations, or to any restricted information, data, or computer databases with sufficient reason to believe that such restricted information, data, or computer databases so obtained may be used to cause or be likely to cause danger to the nation.

Punishment for the act can be imprisonment which can exceed life imprisonment, so more comprehensive legislation has to be formed so that the problem can be tackled efficiently

Other legislative steps include section 69A of the IT Act which gives the central authority to block content online in the defense that it is in the interest of the state i.e., sovereignty and integrity of the country. The person who fails to comply with the directions issued will be liable for imprisonment for a term of 7 years or also punished with a fine[9] and section 70B of the IT Act 2000 directs the government to constitute an emergency computer response team, the rules for the same is provided in the IT rules of 2013 for the nature and size of the unit required.

CONCLUSION

The general population must be made aware of the dangers of the cyber world and also seeing the situation in India, the government must introduce laws to combat cyber terrorism which would in term come in the ambit of a breach of data privacy because this information which can be

[8] The Centre for Internet and society, https://cis-india.org/internet-governance/resources/section-66f-of-the-i-t-act-2000 30 June 2023 2;15pm.

[9] Lawyered https://www.lawyered.in/legal-disrupt/articles/what-cyber-terrorism/ 1 July 2023 2:15pm.

dangerous to the individual as it can affect the security of the nation and cyber-attack has an element of psychological impact more than a physical impact we can combat the issue of cyber terrorism by mainly with creating awareness among the public, the modification of rules in the cyberspace is mandatory. The modern world will not and cannot be free from the cyber world as this is an important part of survival but the wide use of cyberspace makes India more vulnerable to such attacks so the government should take responsibility to ensure the vital data is not misused and it is protected.