Cyber Crimes against the State: A Study on Cyber Terrorism in India

Dr.T. Ambika
Assistant Professor, School of Law, Sathyabama Institute of Science and Technology, Chennai.
E-mail: dr.t.ambika@gmail.com

Dr.K. Senthilvel
Assistant Professor, Faculty of Law, SRM Institute of Science and Technology, Chennai.
E-mail: dr.k.senthilvel@gmail.com

Received May 14, 2020; Accepted July 20, 2020
ISSN: 1735-188X
DOI: 10.14704/WEB/V17I2/WEB17016

Abstract

The computer and network are utilized each and every aspect of humans wherein the internet gives equal opportunities for every aspect of human development. As the client of the internet becomes progressively differing and the scope of online communication extends, there is development in the digital violations for example break of online agreements, execution of online torts and violations, and so forth. The development of computer technology has many times proved that individuals and some groups in the country are using computer technology to threaten international governments and citizens of a country. This research paper clarifies the different types of cyber crime descriptively and particularly analyze cyber crimes against the state.

Keywords

Cyber Space, Cyber Crimes, Cyber Terrorism, Cyber Crimes against State, Cyber War, Cyber Terrorism in India, Indian Law on Cyber Terrorism.

Introduction

"Communication technologies free us from the constraints of the empirical world, we can communicate instantaneously with anyone from anywhere".[1] "Technology eliminates the need, and indeed the ability, to focus on specific, localized activity. This produces a new type of social organization: the network".[2] Being arranged in a physical domain, certifiable wrongdoing has four significant qualities: physical constraints, proximity, patterns, and scale. It doesn't require physical nearness among casualty and culprit. "Cybercrime is unbounded crime, the victim and perpetrator can be in different cities,

states, or countries".[3] One of the key components that keep most individuals from any general public legitimate is the prevention factor, the dread of being gotten and consciness. These standards are changed by the internet because the internet offers criminals a chance to attack his victims from the remoteness. Further, the consequences of criminal activities also are not clearly interpreted. Therefore, it is in need of redefining State laws to counter cybercrimes.

Cyber Terrorism

Cybercrime can essentially be its utilization to encourage traditional crime, for example, robbery, theft, misrepresentation, or a strategic strike, hacking a caution framework before the unapproved section. All of this is possible at the individual, government, or nation-state level. On account of a country attack, there will be no law or law regulating agencies on the world equipped for providing a fruitful outcome; the main concentration leads to political, economic, or military Coercion.

Cybercrime may be "cyber only" violations, for example, spreading of unlawful pictures, documents, or delicate data. Furthermore, proficient programmer bunches additionally fall into this class; they offer digital explicit products and ventures to anybody, from obscure people to governments, that incorporate disavowal of-administration assaults and responsibility for traded off systems. Later on, as a greater amount of our lives come to pass on the web, the cyber only type of wrongdoing will just develop. Perforce, this development will keep on pushing law implementation ever further into the internet.

The unfathomable, topsy-turvy intensity of computers, systems, and computer hacking is as accessible to lawbreakers all things considered to any other individual. Today like never before, non-state on-screen characters have the instruments they have to challenge the position and to be sure the matchless quality of a country. "Pakistani Cyber Army" hacked, damaged and shut down the website of the Central Bureau of Investigation (CBI) in2010.German Police identified that servers used to find genuine lawbreakers and psychological oppression suspects have been entered following a fruitful phishing assault in 2011.

Cyber Activism

From the beginning, countries have delighted in close syndication on the utilization of brutality, and the capacity to align International tension. However, in the advanced telecommunication period, anybody can participate in the international system and this created a very big headache for sovereign states. Any individual can partake in universal

clash—either through the dispersal of publicity or by computer hacking—without answering to any legitimate institution. Consequently, one entrancing part of contention in the Internet period is the wonder of "devoted programmers" who apparently wage cyberwar in the interest of their countries, if not their administrations. As a classification of programmer, activists will ordinarily not have the capacity to utilize the progressed digital assaults that are normal for a country state. Be that as it may, what they help have in out is dynamism. Singular on-screen characters can work spontaneously, and react rapidly to continuous occasions in the universal field. Conversely, government organizations are famously awful at suddenness and adaptability. So with digital activism, the general advancement of an assault might be determined less in the innovative modernity of the assault, and more in the shrewd and eccentric manners by which the digital assaults unfurl.

Cyber Terrorism

Somewhat, all progressed modern economies have gotten reliant on the Internet, and would give off an impression of being defenseless against digital fear based oppression. In any case, in 2013, there is still no obvious instance of digital fear mongering. For the occasion, most non-state psychological militant associations likely despite everything dread nation-state observation more than they trust the unsure possibilities for digital fear based oppression. It is not clear that no instances of digital fear mongers causing genuine physical harm or human setbacks by means of the Internet. Be that as it may, likewise with associations or ethnic groups, terrorists groups are happy with the communications technologies to enable them to organize, select, fund-raise, and disperse promulgation. Around the world, the general degree of polished skill on the digital barrier has risen impressively. The capacity of the country to protect its digital locale is consistently improving. For digital fear-mongering, would-be cyber terrorismmay require some degree of state sponsorship.

Information Technology Act, 2000 on Cyber Terrorism

The Information Technology Act defined cyber terrorism and contemplates two broad categories through which cyber terrorism may be caused. The Supreme Court has stated about the difficulty in defining the definition in *Hitendra Vishnu Thakur v. State of Maharashtra,*

“terrorism has not been defined under Terrorist and Disruptive Activities (Prevention) Act, 1985 (TADA) nor is it possible to give a precise definition of 'terrorism' or lay down what constitutes 'terrorism'. It may be possible to describe it as use of violence when its

most important result is not merely the physical and mental damage of the victim but the prolonged psychological effect it produces or has the potential of producing on the society as a whole".[4]

Cyber Terrorism in India

Digital and data innovation are a lot of utilized by fear mongers in India for assault against the country. Phone, cell phone, remote, computer offices are accessible wherever in India. That is the reason the terrorists can speak with one another in any event, being in the remote regions. They can control the whole gathering exercises from remote regions. These days the majority of the terrorists have their own sites.

India ranked as 2nd in cyber attacked countries in the year between 2016-2019. it is evident that 22 percent increase in cyberattacks in India on IoT deployments. It happened in 2nd time further India faced large number of assaults in the many departments.

It also exposed that Bengaluru, Mumbai, and New Delhi faced the large number of cyber-attacks in the Indian cities. India is in fourth place of the top ten notable countries in the world for cyber-attacks. In report of India Today, "Chennai identified as the highest 43 percent of cyber-attacks in the beginning of2019."[5]

Report of Annual Cyber Security by CISCO explains that "53% of cyber-attacks rooted more than $500K of financial loss to Indian organizations in 2018. India faced an increase of 7.9% in data breaches from 2017. the average cost per data breach record is increasing to Rs.4,552" [6]

The Hacking Tendency of Terrorists

Terrorists are inspired for hacking and damaging of sites in India, Pakistani Hackers' Club (PHC), G-Force Pakistan, Hostile to Indian Crew (AIC), Pro-Pak Hackers are terrorists.

On 10 January 2001, Mr. R.K. Ragavan (the then Director of CBI) said that "various instances of hacking of Indian web destinations have been followed to Pakistan however it is hard to nail them. In July 2005, there were 635 episodes of breaking Indian internet sites."[7]

The occasion in which seizing of Indian Airlines trip to Kandahar in Afghanistan in December 1999 is one of the activities of cyber terrorism in India because the terrorist

groups conveyed the commands and controlled the entire activities through communication networks however it had stayed undetected.

G-Force is one of the Hackers Group it distributed the message against the Indian government. They additionally had mutilated and hacked a few web sites of Indian Government, organizations and logical associations.

Bhabha Atomic Research Center (BARC) websites had hacked by hackers belong to western countries to steal the information relating to Pokhran-II atomic test in the year 2001. In May 2001, the Government of India and E-Business divisions of India started to act against Pakistani hackers. The indictment of DoS and personnel computer worm assaults presents genuine difficulties to most criminal law frameworks, assaults may not include any physical damage on personnel computers. The essential need to control cybercrime, the subject of whether the anticipation and indictment of assaults against basic framework need a different authoritative methodology is being talked about. To accomplish this objective Government established power on cybersecurity.

As per the Cyber Security Force, this isn't the assault for the wellbeing of attack rather it is a message to pass on that India likewise can do. India is mentally influenced by hack assaults by Pakistan. Consequently, opening the source codes of Pakistan's sites was taken as an approach to forestall and control digital psychological oppression in India.

"In June 2001 the Pakistani Hackers Club defaced Indian website for showing disrespect to the Indian flag."[8] The concentration for cybersecurity had been very poor in India. Organizations had spend just 0.8 % of their data innovation spending yearly as against the world normal of 5.5 %.[9] In April, 2009, Chinese digital covert agents hacked into government frameworks utilizing Ghostnet in 103 nations, which incorporated the PC organize that was utilized by Indian Embassies abroad and the frameworks of Dalai Lama.[10]

Attack on the Indian Parliament

The computer was seized from terrorists, who attacked Indian Parliament on 13th December, 2001, the seized computers was sent to the Computer Forensics Division of BPRD. Computer Forensics Division discovered that they got to the web through Pakistan based ISPs. Exploring officials likewise discovered approaching and active wireless call quantities of terrorist groups which were a lot of accommodating for the police

examination. Police likewise discovered a satellite association with expired terrorists' mobile phones. [11]

UIDAI Aadhaar Software Hacked

In 2018, nearly 210 websites of Indian Government had leaked Aadhaar details of people. It is a huge data breach of personal information because of nearly 1.1 Billion Indian Aadhaar cardholder's details made available online. Aadhaar Number included bank account numbers, IFSC codes, driving license details PAN, Ration Card details, Passport details and mobile numbers, Therefore, every personal information of every individual was leaked. Whoever may get any individual Aadhaar details from many private sources.

Cyber-Attack in Cosmos Bank at Pune

The cyber attack held at Cosmos Bank in Pune in 2018. In this hacking, hackers siphoned off Rs.94.42 crore from the Cosmos Cooperative Bank, Pune. This incident had alarmed the entire banking sector of India and made them afraid. In this attack, hackers hacked the ATM server of Cosmos Bank and stole information about RUPEE and VISAS debit cardholders. Hacker gangs from around 28 countries had taken the Money. Money was wiped off when withdrew the amount as early as they were aware.

Canara Bank ATM Servers Hacked in 2018

Cyber attackers targeted Canara bank ATM servers and steal details of debit cardholders. skimming devices are used by hackers to had stolen the details of more than 300 users. Money was taken from stolen details of debit cardholders from the maximum amount of Rs.40,000. Nearly20 lakh rupees had been wiped off from 50 debit cardholders in 2018.

SIM Swap Scam

In August 2018, two hackers of Navi Mumbai arrested for illegal transfer of Money from other individual bank accounts. Through fraudulently collecting SIM card details, hackers blocked SIM cards of individuals' and with the usage of fake documents and posts, they carried out transactions through online banking. In this way, hackers transferred Rupees 4 crore from many individual's bank accounts. The hackers also planned to stole the details of accounts of various notable companies.

Attack on Indian Social Insurance Website

In 2019, healthcare websites in India have been hacked it becomes a victim of cyber-attack. In this attack, hackers hacked in and invaded a leading the social insurance website based on India. Like as specialists, the hackers stolen the records of 68 lakh patients.

Hacked on Indian News Websites

Two people groups hacked websites of two Indian news agencies like Zeenews.com and India Today.com and websites were down for an hour. Both the goals The ambush quickly blocked access to a couple of India Today locales, anyway no of its news goals. After their websites were hacked Zee News and India Today are evaluated and improved their computerized security.

Conclusion

Cybercrime by their very nature are multi-dimensional and complex. As cybercrime dynamically advances into a sorted out movement, the thought processes of gatecrashers are not, at this point restricted to taking data just, however conceivably disturbing business or direct surveillance in the interest of contending associations. Despite the way that Institutions understand the need to protect their IT establishment, cyber terrorists have normally been a step ahead at mishandling new vulnerabilities in IT structures and the methodology of their goal. Clearly, target affiliations have been found requiring concerning countering these cyberattacks, especially at the National level.

What's to come is obscure, yet this section has indicated that the intensity of PCs and PC systems is being abused by everybody—including spies, hoodlums, activists, psychological militants, and fighters. There are known, away from of digital assaults that have been utilized to encourage undercover work, wrongdoing, activism, fear based oppression, and war. Later on, as the Internet extends its venture into each part of our national and common social orders, and as we naturally develop our reliance upon it, the quantity of digital assault models, just as their possible effect on our lives, is probably going to increment. At the individual level, we should stress over opportunity and protection. At the national level, chiefs will stay concentrated on wrongdoing, psychological warfare, war, and transformation. Could digital assaults down a force matrix or a money related market? In principle, yes … practically speaking, we despite everything don't have the foggiest idea. Regardless, we do understand that the Internet outfits governments with an incredibly necessary resource for controlling our lives, and to lead perception against their adversaries, yet against their own inhabitants. As needs are,

in the Internet era, it is fundamental that governing bodies place a growing complement on respect for both the standard of law and the Laws of cyber attacks.

Care getting ready projects set up for key agents in high-risk domains is an astoundingly strong instrument in preventing cyber attacks. Typical checking and passage testing are structures that are used to thwart ambushes. Lastly, activities like end-point workstation security and PC can help forestall assaults by means of online.

References

Brenner, S.W. (2002). Organized cybercrime-how cyberspace may affect the structure of criminal relationships. *NCJL & Tech.,4*, 1.

Ronfeldt, D., & Arquilla, (2001). J. Networks, netwars and the fight for the future.

A Report of the President's Working Group on Unlawful Conduct on the Internet, The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet (2000) https://www.hsdl.org/?view&did=3029

(1994) 4 SCC 602 Hitendra Vishnu Thakur v. State of Maharashtra.

Report ofIndia Today, Dec 23, 2019.

Annual Cyber Security Report of CISCO.

The Hindu, Chennai, 2nd July, 2005

The Times of India, Kolkata, 23rd July, 2005.

Tribune News Service, Ludhiana, Chandigarh, India, 30th June 2001 News publication.

Thaindian News, Chinese hack into Indian embassies, steal Dalai Lama's documents. 29th March, 2009.

Veer, S., & Bharat, B.P. Cyber Crime and Need for National and International Legal Control Regimes. *Punjab University Law Review*, 44: 24.