Review Article

Journal of Social Welfare and Management
Volume 12 Number 4, October–December 2020
DOI: http://dx.doi.org/10.21088/jswm.0975.0231.12420.3

The Stringent Study on Cyber Defamation & Cyber Terrorism

Saniya Sharma

How to cite this article:
Saniya Sharma/ The Stringent Study on Cyber Defamation & Cyber Terrorism J. Soc. Welfare Manag. 2020; 12(4):145–152.

Abstract

The advent in the cyberspace has revolutionized in terms of connecting & interacting globally. The accessibility, secrecy, accountability, integrity, seclusion of one's own space, and the interactive, responsive nature of communications over the web has made the users far less inhibited than before especially about the contents of their messages.[15] The web has made it far easier than ever before to disseminate defamatory statements to a worldwide audience with impunity. Also committing terrorism over cyberspace has become more sophisticated with time. There have been proposed several provisions under Indian Penal Code & IT Act, 2000 for cyber defamation as well as several convictions have been made for cyber terrorism.[12,13] India is well aware of the devastating effects of cyber attack and has thus implementing audacious measures to improve its security structure.

Keywords: Accessibility, Cyberspace; Cyber terrorism; Cyber defamation; Indian Penal Code; IT Act 2000.

Author's Affiliation: 1st year MSc Student of Forensic Sciences, Chandigarh University, Punjab 140413, India.

Coressponding Author: Saniya Sharma, 1st year MSc Student of Forensic Sciences, Chandigarh University, Punjab 140413, India.

E-mail: saniyasharma4200@gmail.com

Introduction

Due to the advent of computer & internet the operation of science & technology has completely revolutionized. The unbelievable speed, an incredible accuracy, eradication of drudgery of work & cost effectiveness has made the computer & similar devices indispensible to all concerned.[14] The unstoppable growth of the internet has brought an evolution in the field of communication & have created a separate but huge space for expressing opinions, thoughts, feelings globally. But this increase in the medium of communication has led to enormous chances of risk occurs due to the abuse of mediums of communication. Removal of such barriers to freedom of interaction has provided unfettered capabilities, to people who post unnecessary, unethical, gratuitous, false statements about a person, community, company, religious groups, politician in order to harm their goodwill & reputation. Such an act is termed as Cyber defamation.[1] Apart from cyber defamation, most heinous among all is the cyber terrorism that is the major threat revolving over the countries & for that all possible tools, methods & most importantly technology has been the major weapon from the past years. Cyber terrorism is basically, anti national activities that formulates well planned & an organized use of technologies by cyber experts that resides inside & outside the country.[5] It employs the use of information technology to organize & execute attacks against computer, network, and telecommunication infrastructures, for exchanging information or making threats electronically.[5]

Cyber Defamation

It is basically referred as an act of defaming, errant, abusing or an act of incommode caused to a person, company, organization etc in order to mortify or destroy ones reputation. Under the section of 499 of Indian penal code, defamation has been defined as "whoever, by words either

spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person is said to defame that person".[12] By the same token, doing such act on cyber space leads to cyber defamation or online defamation.

Classification of Online Defamation

Defamation can be classified into two groups-

- Libel - Publishment of any defamatory material in written form.[1]
- Slander- Publishment of any defamatory material that is stated verbally.[1]

Authors of e-mail, content provider of website, who are the primary publisher of defamatory material in cyber space, are liable to such cases of online defamation & also bulletin board operator because it's there bounden duty to check the content before it is being available to public. However according to the section 79 of IT act 2000, an intermediary shall not be liable if it does not modify or initiate such content but solely acts as a facilitator.[13]

Breach of Conduct of Cyber Defamation

The breach of conduct that has been a part or that comes under online defamation are as follows

- **Scoffing any person on cyber space**

  When a person deride another person, community, batch by tagging them in incommode post, messages, comments & even like and share such post on any of the social networking site then he must be in trouble as serious action will be taken against him/her under the following laws

a. Section 499 of Indian Penal Code- for Defamation.[12]

b. Section 66A of Information Technology Act, 2000- for sending offensive electronic messages.[13]

- **Scoffing any Minister**

  It is completely unethical to ridicule any of the government officials by messages, comments, post & even liking & sharing such post on any of the social networking site & stated them as a corrupt politician even when he is not finding guilty by the court of law still doing that in order to harm their reputation is an offensive act and is illegal under the following laws-

a. Section 499 of Indian Penal Code- for Defamation.[12]

b. Section 66A of Information Technology Act, 2000- for sending offensive electronic messages.[13]

c. Section 124A of Indian Penal Code- for Sedition.[12]

- Tagging on pornographic posts

  Tagging any person on obscene photos intentionally or unintentionally is unethical and if a person who is facing problem or whose reputation is being damaged due to that then he/she has the right to file a case against the person who tagged him/her as it is an offensive act under the following laws.

a. Section 499 of Indian Penal Code- for Defamation.[12]

b. Section 66A of Information Technology Act, 2000 - for sending offensive electronic messages. [13]

- **Using abusive words on cyber space**

  As we have seen this is the most common thing happened to every other person on cyber space, on any of the post some anonymous person used to send abusive messages or made abusive comments that leads to destroy ones image has been subjected to punishment under the following laws.

a. Section 499 of Indian Penal Code- for Defamation.[12]

b. Section 66A of Information Technology Act, 2000- for sending offensive electronic messages.[13]

- **Creation of erroneous accounts**

  When any fallacious accounts or documents have been created just to harm ones reputation then this is punishable under- Section 469 of Indian Penal Code- for Forgery.[12]

Case Studies

SMC Pneumatics (India) Pvt. Ltd. vs. Jogesh Kwatra.

It was the first ever case of cyber defamation reported in India. Here, Jogesh Kwatra the defender, was himself the employ of plaintiff company had

accused for sending obscene, derogatory, vulgar, filthy, defamatory, intimidating , humiliating & abusive emails to his employers as well as to the different subsidiaries of the company around the world. The purpose behind it was solely based on defaming or tarnishing the brand image & jeopardizes the reputation of Managing director of company, Mr. R.K Malhotra. The emails sent also resulted in infringement of legal rights of plaintiffs as being the employee of the company he is bounded by the duty of not to send such emails to anyone.[3]

It is pertinent to note that after becoming aware of the action caused by defender his services were terminated.

Facts

In 2014, plaintiffs for seeking perpetual injunction moved to Delhi District Court but due to the insufficient & lack of locating appropriate electronic evidences that could be admissible in the court under the section of 65A & 65 B of Indian Evidence Act, 1872.[16]

Thus it was difficult to form any direct or indirect link in concluding him as the one who was sending the emails. However, ultimately the case was gone in the favor of the defendant.

Judgment

After hearing the detailed arguments of plaintiff's counsel, Hon'ble judge of Delhi High Court passed an ex-parte ad interim injunction noticing the fact that prima facie case had been made out by the plaintiff. Subsequently, the defendant was restrained by the court for sharing or sending obscene, abusive, derogatory stuff in cyber space.[2,3]

This landmark judgment made is prodigious as it paved a way & has laid down the foundation for the development of this offence in the Indian judiciary.

Kalandi Charan Lenka v. State of Odisha

This was the case of 16th January 2017, in which the petitioner is a woman studying in the Pattamundai Women's College at Pattamundai. One day the victim has received unknown obscene messages in her mobile imputing her character & had also come through the cell phone of her father that remorse her father. Then during 2015-16, the father of the victim received written letters that containing sexual remark with an intention to denigrate the character of the victim girl. Also morphed naked picture was posted on walls of the hostel where the victim stayed.

Judgment

The issue was investigated by the cyber cell of crime branch and the High Court held that the accused was prima facie liable for sexual harassment offenses under Section 354A, 354D for cyber stalking under the Indian Penal Code, 1860,[12] Section 66-C for identity theft, Section 66-D for impersonation and Section 67 and 67 for electronic transmission of obscene and sexually explicit content. Hence, the application for the bail was also rejected.

Swami Ramdev & Anr. v. Facebook Inc. & Ors

In this case, Priyanka Pathak Narain published a book titled 'Godman to Tycoon – the Untold Story of Baba Ramdev'. Swami Ramdev who is a public figure challenged the contents of book as defamatory in Karkardooma District Court. This book being a part of separate litigation had been restrained from being published as the court held that it constitutes prima-facie defamatory content on Baba Ramdev. But the petitioners, contested that since the content in question could be accessed from Facebook, Google, You-tube, twitter thus a global blocking order ought to be passed.[10]

Facts

Plaintiff claimed that once a defamatory book or article was published, then the publisher of that book was liable for defamation. They argued by giving various statements that there was nothing in the IT Act which stopped courts from giving global take down orders.

Defendants (Facebook, Google, You-tube, Twitter)- claimed that these platforms were not publishers but mere intermediaries & thus not liable for third party content on their websites. Sec. 75 that provides for extra territorial jurisdiction was limited to infringement and offences under the IT Act and defamation wasn't covered by these provisions. Geo-blocking of content specific to India would be sufficient to take care of plaintiff interests.[10]

Judgment

Chief Justice Pratibha Singh had passed an order to eliminate all defamatory content posted online against Baba Ramdev, without any territorial limit, stating that if the content is uploaded from India or such content is located in India on any computer resource, then the Courts in India should

have international jurisdiction to pass worldwide injunctions.[10]

Gurugram teen suicide- Pressure of defamation

A 17 year old boy, Manav who was the 12th standard student of Heritage school Gurugram jumped from the 11th floor of his apartment & laid straight on the road below & ultimately lost his life. This case came into light when already the bois looker room was on highlights. Two days ago before his death, a girl shared a post on instagram stating that she has been molested & raped by Manav two years back when he was 14-15y/o. She claimed a story without any factual proof, accused a teen with the attempt of defaming him.[2]

Facts

It was the time when bois locker room controversy was already ignited & this too got viral within fractions because of that Manav received many threat calls & messages & were also harassed by that girl & her mates. He tried hard to convince the people around, that he was innocent but the constant threats plus the dishonor & defame it brought along was unbearable & impotent. Due to which he had panic attacks and was under tremendous pressure & impulsively decided to commit suicide.[2]

Outcomes

Because of an allegation over social media that might not be authentic has taken a child's life & shattered the family. His father claimed that the allegations were "defamatory & slanderous". The local police investigated the case & stated that they have seized the mobile phone of deceased & has sent to forensic examination.[2]

National union of bank employees vs. Noorzeela binti lamin

In this case, some defamatory content were posted to all the defendant's friends over Facebook & to all others who could have access to view the Facebook page of defendant & due to the era of networking the comments of defendant which must have read by her Facebook friends were having possibility to be in turn read by their friends too, depending upon the privacy settings.[2,4]

Facts

Plaintiffs claimed that reading such comments posted by the defendants, would make people think that the plaintiff is a dishonest union that cheats its own members, having their own agendas & also that the plaintiffs can even misappropriates the monies. However, they stated that their reputation has been tarnished because of such derogatory messages & comments.[2,4]

Outcomes

The court opined that harming anyone's reputation is a matter of serious concern & has ordered the defendant to make a halt on publishing such defamatory content and allowing similar libels to be published in future.[2,4]

Cyber Terrorism

Traditionally terrorism is defined by Federal Bureau of Investigation, as an unlawful use of violence against person, property to intimidate the government, civilians, or any segment in furtherance of political or social objectives. Thus, in cyberspace cyber terrorism can be defined as "use of computer resources to coerce others.[5,6]

After the September 11 attacks, on world trade center it is pertinent to note that terrorism has reached to a new level of sophistication. Using network in an incredibly effective fashion as weapons for intimidating or coerce against the civilians by gaining the access to physical resources without the usage of any traditional approach. The internet is a virtual encyclopedia of information that terrorists can use to carve a framework to execute such cyber attacks by tampering the original data, hacking the information or data theft & communicating it to procure the resources.[5,6]

Modus Operandi Opted for Cyber Terrorism

- Secret writings/Cipher/Code-

  For safe communication, "Al Qaeda Training Manual" is one of the many evidences encountered from terrorist organizations.
- Denial of services.
- Sending threatening emails.
- Defacing of the government websites.
- Hacking of crucial or protected systems of government.
- It could affect the computer & network as a whole.
- Mostly done by hi-tech computer experts (offenders).[5,14,15]

Case Studies

WannaCry, 12 May 2017

This ransomware attack was unique in its own because of its nature & delivery. It was one of the most widespread attacks, exploiting leaked window software vulnerability by encrypting the data & demanding payment in bitcoin. This wannacry was basically a 'worm' that is self replicating as like viruses that gets attached to a particular host & replicate themselves & then contaminate the network & other devices it is in contact with.[5,6]

Facts

This wannacry infected more than 2,30,000 computers in over 150 countries within one day. Many sections of National Health Service (NHS) got infected causing hospitals & GP surgeries to run their services on emergency- basis during the attack & demanded payments of between $300-$600 to restore access.

Windows released a series of patches that repaired the SMB(server message block) vulnerability, just one day after the attack. Days after the attack the researchers found that registration of "kill switch" domain name prevented the execution of encrypted file. Also with the time attackers released another version of it that was named as 'wannacry with no kill switch'. But after days of immense struggle "Adrien Guinet" carve out a way to retrieve the RSA key from malware files, halting the execution of the attacks & spreading of heinous wannacry attack.[5,6]

Judgment

United States & United Kingdom were the two major states badly hit by wannacry. In US such malware attacks that cause terror are considered illegal under Computer Fraud & Abuse Act(1984). Such conviction for cyber crime carries 10 years of imprisonment with a huge dollar amount. In UK such attacks are considered under Computer Misuse Act(1990) that involves conviction of 14 years sentence in prison. Due to plentiful cyber crime legislation still this is not sufficient in controlling the globally threatening cyber attacks. In this case also, security researchers after investigation figured out that it could be having North Korean origin. They laid out the fact that substantial commonalities in the tools, techniques, & infrastructure used by attackers of wannacry & that used by the Lazarus group that has been tied to North Korea. Attacker's identity was never revealed except Park Jin Hyok & even none of them have gone to prison or had trials. Even Park has been charged in absentia, with US Federal arrest warrant.[5,6]

9/11- Root cause, The Cyberspace.

On September 11th 2001, terrorists hijacked planes & deliberately flew them into major landmarks in America killing thousands of civilians. The 19 attackers trained by al-Qaeda, had been planning and coordinating the attack for years. 9/11 attack has now been marked as the anniversary of one of the worst terrorist attacks on American soil in US history.

Facts

Osama bin laden leader of the militant Islamic organization al-Qaeda instigated the attacks. Khalid sheikh Mohammed often referred to as "KSM" was allegedly the key operational planner. Both Osama & KSM met in Tora Bora, Afghanistan in 1996 where KSM presented proposals of attacks on 9/11. At 8:46am, the hijackers crashed the first plane into the World Trade Center's North Tower & at 9:03am, another plane flew into South Tower. The root cause of the attack was cyberspace i.e. it was through network because of which signals or messages were transmitted for functioning or initiation of the attack.

Outcomes

Before this attack, no country was ready to face the dangers of cyberspace, and the massive impact it carry along. The US then decided to take impulsive measures to cope up with the cyber security threats that can spread terrorism like 9/11. It was claimed that if strong measure were implemented for cyber security and strong provisions if universally accepted then such cyber terrorism could be halted & justice could be provided.

Stuxnet, 2009

It is a highly developed computer worm that exploits multiple previously unknown Windows zero-day destructibility's to infect computers & the devices connected. The aim of this sophisticated worm was to target Iran's nuclear programme mainly through hindering their facilities to function, all this while acting in complete secret. It aimed to sabotage Iran's programme in a way that eradicate its existence by causing damage to their uranium enrichment program in such a destructive manner that would halt President Mahmoud Ahmadinejad from creating a potential nuclear weapon.[7]

Facts

A report conducted by Siemens cyber-security experts declared that Stuxnet was found in America, Australia, parts of Africa and all over Europe. Despite that, over 60% of the cyber-attack was targeting Iran alone.[7,8]

Outcome

In relation to the facts, the malware i.e. Stuxnet destroyed the 1000 Iranian nuclear centrifuges, made it rather evident that the sole purpose of Stuxnet was to sabotage the development of Iran's nuclear program. Both security experts and diplomats have stated that Israel and Western governments believes that one of the most effective ways for slackening the Iranian nuclear program is through vandalizing it & preventing them to make a highly potential nuclear weapon. The agenda behind it was clearly political & In 2012, it was reported that this worm was specifically developed to spread terror in Iran by US & Israeli forces that faked as industrial accidents.[7,8]

Ukrenergo blackout, Ukraine, 17- 18 December 2016

In 17-18th December, 2016 a power cut hit hard to the parts of Ukrainian capital, Kiev had encountered cyber-terrorist attack claimed by researchers after investigating the incident. This incident was then linked with the hack & blackout in 2015 by the cyber security company ISSP (Information System Security Partners).[17]

Facts

The national energy company Ukrenergo stated that the 2016 power cut had amounted to 1/5th of Kiev's power consumption at that time. Outside the capital it affected the Pivnichna Substation & left the people in the city without electricity. As for the 2015 attack on regional electricity distribution company which was blamed on Russian security services. Later investigation revealed that almost the 2015 & 2016 attacks were same with a single distinction that the 2016 was more organized & complex from 2015.[17]

Outcomes

Petro Poroshenko, the president of Ukraine in December passed a statement during the meeting of National Security & Defense Council that "Acts of terrorism & sabotage on critical infrastructure facilities remain possible today via cyberspace". Investigation of tons of incidents occurred in last 2 months of 2016 indicated the complicity of Russian security services either directly or indirectly.[17]

26/11

26/11 was one of the major cyber terrorist attacks India has encountered that lasted 4 days across Mumbai. After investigation it was demonstrated that digital correspondence between the psychological militants and use of digital innovation by them in order to get familiar with the natives and the place, made comparable sabotage brings about India.

Implementation of web for tracking & clog the endeavours of Indian commandos.[18]

Facts

Because of lack of cyber security measures at that time the terrorists were able to make a complete framework & also communicate it through the networks that appeared latent to the security services. Due to which terrorist group stormed buildings in Bombay, killing 164 individuals. 9 of the gunmen were killed throughout the attacks. Beginning from Karachi, West Pakistan to Bombay via boat, who meanwhile hijacked a fishing trawler and killed four crew members, throwing their bodies overboard. The terrorists docked at the Bombay city district & led to the devastation.[18]

Outcomes

The attackers used a satellite phone and cell phones to interact with fellow members moreover as their handlers that were primarily based in Pakistan. It was revealed that every plan of action, knowledge of the native, security system was shared between the attackers & their handlers over cyberspace. 26/11 was one of the most threatening incidents of our country which made the government aware of the cyber security and cyber threat and major steps that should be taken for it.[18]

Several Conventions for Cyber Terrorism

For the issue of cyber terrorism conventions applied are as follows[6,11]

- 1963-The Convention of offences and certain other acts committed on Board Aircraft,
- 1970- The Convention for the Suppression of Unlawful Seizure of Aircraft,
- 2010 Protocol - Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft,

- 1971- The Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation,
- 1973- The Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons,
- 1979- The International Convention against the Taking of Hostages,
- 1980- The Convention on the Physical Protection of Nuclear Material,
- 1988 Protocol –solely for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation,
- 1989- The Supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation,
- 1988- The Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation,
- 2005 Protocol- To the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation,
- 1988 Protocol- For the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf.[6,11]

Conclusion

From this review paper I can surely conclude by stating the fact that "With great power comes a great responsibility". The phrase is the true paragon of the current scenario of use of technology & the potential misuse.[11] Due to the advent of technology, it has become a tremendous source of communication and a means of connecting globally but simultaneously a platform of committing heinous crimes by just giving a single click.[14] The cyberspace has now been considered as an integral part of living. It is a platform to share ones feelings, opinions, perspectives but at the same time it becomes very important to take care of other feelings too.[14,15] Though our constitution provides freedom of speech & expression but it should be surrounded with or having certain boundations that will safeguard the interests of sovereignty and integrity of India, interest of decency, morality & also in relation to defamation. The case of cyber defamation and cyber terrorism are the major threats India is facing over cyber space. A single trolling over social media handles can become the cause of tarnishing someone's reputation.[9] With the emergent nature of the digital economy, cyber tools, and the capabilities of our own adversaries require a repeated reassessment of cyber attack over time.[14] Though there are several provisions under IT Act 2000, IPC still due to the lack of acceptance of universal law for cyber crime doesn't grant the necessary justice to the deceased.[11] Due to the severe cyber attacks that the country has faced, the government has taken and considered prominent measures to improve the security structure of the country.[11,15]

References

1. Cyber Defamation, can be retrieved from: http://www.helplinelaw.com/docs/main.php3?id=CDII2
2. Do the Facebook related laws violate the constitution of India – Rohas Nagpal, 12 Sep, 2013 can be retrieved from : http://www.facebooklaw.in/do-the-facebook-related-lawsviolate-the-constitution-of-india/
3. Cyber Defamation in Corporate World – Pradhumna Didwania, 31 January, 2013 can be retrieved from: http://www.mondaq.com/india/x/218890/Social+Media/Cyber+Defamation+In+Corporat e+World
4. Online Defamation & various Legal Issues – Vibhor Verdhan, 4 Sep, 2009 can be retrieved from: http://www.legalserviceindia.com/article/l380-Online-Defamation.html.
5. Cyber Terrorism– Global Security Threat, International Scientific Defense, Security and Peace Journal 327.88:004.738.5-027.22 scientific article.
6. Cyber Terrorism: Assessment of the threat to insurance article
7. Alvarez, Joshua. Stuxnet: The world's first cyber weapon. Center for International Security and Cooperation, Feb 3rd, 2015 http://cisac.fsi.stanford.edu/news/stuxnet
8. Borger, Julian. The truth about Israel's secret nuclear arsenal. The Guardian, Jan 15th, 2014 https://www.theguardian.com/world/2014/jan/15/truth-israels-secret-nuclear-arsenal
9. Trolling-cyber-harassment-and-defamation-Know Your Rights article.
10. India-delhi-high-court-orders-removal-of-all-posts-defamatory-to-Ramdev-article.
11. India-revisiting-the-current-scenario-of-the-safeguards-for-cybercrime-article.
12. Collin, B. (1996). The Future of Cyber Terrorism. Proceedings of 11th Annual International Symposium on Criminal Justice Issues, The

University of Illinois at Chicago Indian Penal Code, 1860 –Indiankanoon.

13. Information Technology Act, 2000- Indiankanoon.
14. Hannan.M & Blunde;. B (2004). "electronic crime- it not only the big end of town that should be worried"' we-B centre & edith cowan university, PP 1-9
15. Muthukumaran.B (2008), "cyber crime scenario in India", criminal investigation department Review, January, pp. 17-23.
16. Indian Evidence Act, 1872.- IndianKanoon.
17. Ukraine's power outage was a cyber attack: Ukrenergo, By Pavel Polityuk, Oleg Vukmanovic and Stephen Jewkes.
18. Journal Media and Communication Studies Vol. 1(6) pp. 095-105, December, 2009, The print media coverage of the 26/11 Mumbai terror attacks: A study on the coverage of leading Indian newspapers and its impact on people by M. Neelamalar*, P. Chitra and Arun Darwin Department of Media Sciences, Anna University Chennai, Tamil Nadu, India