INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

www.ijlra.com
Volume 2 Issue 7 | Jan 2024
ISSN: 2582-6433

CYBER TORT LAW: EXPLORING THE INDIAN CONTEXT

AUTHORED BY - PURWA BALA[1]

ABSTRACT

Cyber law, a multifaceted crime scene, includes a wide selection of laws, regulations, and constitutional provisions that govern activities in our online world which allow access, creatively manage the progress of access, or online communication The dynamic realm works because the important relationship where technology and law intersect, and it formulates the rights, duties, and responsibilities of stakeholders in the digital realm.

At its core are cyber law and the concept of cybercrime—a term that refers to illegal activities that use computer systems as tools, targets, or in any way These crimes from the traditional corruption of theft, cheating, forgery, and slander to the modern, technologically sophisticated - Push crimes are as diverse as they are, all punishable under the Indian Penal Code but the evolution of the digital age has rapidly led to the emergence of many new cyber threats and specialized crime planning is needed to effectively deal with emerging complex situations
The centrepiece of this legislative approach is the Information Technology Act of 2000, a landmark piece of legislation designed to combat modern cyber threats in general. These basic rules provide a robust framework in online governance for various critical aspects to monitor online transactions, protect digital signatures and strengthen fact security systems Through pure recommendations and regulatory mechanisms by defining, the Code seeks to reduce the unique vulnerabilities of electronic, virtual communications Ensures security, integrity, and reliability.

In complex cyber law, stakeholders have to contend with rapid technological developments, evolving cyber threats, and rapidly evolving regulatory frameworks therefore changes in motion so and innovations in regulatory paradigms are needed to effectively address evolving challenges digital age. As cyberspace redefines human communication and business reasoning, the principles of cyber law are indispensable tools, protecting the interests of individuals, businesses

[1] *Author is a LLM student at IILM University, Greater Noida,* U.P, India.

ISSN: 2582-6433

and citizens in an increasingly connected world.

Keywords *- Cyber Law, Cyber Crime, Cyber Forensics, Information Security, Information Technology Act*

I. INTRODUCTION

The term "cyber" refers to the virtual world of the internet, where there are no limitations between users. The widespread usage and impact of information technology expose societies to potential misuse. The internet gained importance in the mid-1994s, with countries realizing its potential through its rapid growth.

The word "tort" comes from the French language; in English, it is equivalent to the phrase "wrong"; it is derived from the Latin word "tortum," which means "wrong or injury," and the word tortum is derived from the verb "torquere," which means "to twist." It is merely a breach of duty, which results in a civil wrong[2].

A tort is a civil wrong for which a remedy is given in terms of damages, the damages that are paid to the plaintiff (the person who suffers the damage and brings the suit to the court of law) against the defendant (the person who commits the tort against the plaintiff and has to prove his innocence in court) in terms of unliquidated damages. A tortfeasor is someone who commits a tort, and if there are numerous people involved, they are referred to as joint tortfeasors since they are all jointly accountable for the tortious act and can be sued either individually or collectively.

Cyber wrongs are unlawful acts conducted via the internet; the only difference between a wrong and a cyber wrong is that a cyber wrong involves the use of technology in the commission of it, i.e. the medium through which a cyber wrong is perpetrated is through technology.[3]

With the creation of computers and the emergence of the internet, a new type of tort has sprung up, namely cyber torts.

Cyber torts are torts perpetrated in cyberspace. These are extremely significant since they are on the rise and can have serious consequences for society. Everyone in society should be aware of the damage caused by cybercrime because technology has become an integral part of everyone's life.[4]

---

[2] *Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, 61st plenary meeting.*

[3] *Available at: www.scribd.com/document/283532243/ Cyber-Torts last visited on 27th Mar 2024.*

[4] *http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspac e.pdf.. Mark Lander, A Filipino Linked to "Love Bug" Talks About His License to Hack, N.Y. TIMES, October 21, 2000c. 2, 2008) [hereinafter Shanghai Cooperation Agreement].*

ISSN: 2582-6433

Examples of cyber torts include e-mail harassment, cyberstalking, cyber harassment, and cyber defamation.

The internet has brought numerous benefits, including e-commerce, e-banking, endless information, and quick communication. Through email, messengers, voice chat, social media, and other channels. However, there are also negative aspects such as hacking, stalking, and defamation.

The internet has become the primary mode of communication, offering anonymity, reliability, and convenience. It has also become a breeding ground for individuals interested in using the internet for illicit purposes, both financially and otherwise.

The biggest challenge for the law is keeping up with technological advancements. One challenge of creating technology-based legislation is that it may become outdated quickly. Therefore, potential technologies must be formulated in a technology-neutral manner. There has to be consistency between the laws[5].

II. HISTORY OF CYBER TORT

The Internet, which began as the US Défense Department's ARAET, was intended to connect computer networks to various radio and satellite networks. The first legal opinion to mention the Internet was United States vs Morris[6]. The defendant in Morris was a Ph.D. student who distributed an Internet worm that crippled thousands of universities and military systems across the United States[7]. In the same year, Robert Riggs was charged with gaining illegal access to a Bell South computer and misappropriating confidential information about the telephone company's 911 system[8]. He later released this private information in the Hacker newsletter. It was not until 1994 that any plaintiff won in an Internet tort lawsuit. In a contentious case, an anthropologist was refused tenure at the University of Western Australia in Rindos v. Hardwick. A competing anthropologist, Hardwick, made a statement supporting the university's decision and accusing Rindos of sexual deviance and research that is harmful to Australia's aboriginal people. Although an Australian court imposed the first damages award in an Internet tort case, the vast majority of subsequent cyber torts have been handled in the United States[9]. Over the last

[5] *Article named Cyber Tort in the famous American Journal of International Commercial Law and Technology written by 'Gregory C.*
[6] *Mosier' and 'Tara' have been utilized to get the matter on types of cyber-Torts in India.*
[7] *Q. Yeh and A. Chang, "Threats and countermeasures for information system security: A cross-industry study", Information & Management, vol. 44, pp. 480-491, 2007.*
[8] *An article named Cyber Tort in the famous American Journal of International Commercial Law and Technology written by 'Gregory C. Mosier' and 'Tara' has been utilized to get the matter on types of cyber-Torts in India.*
[9] *International Court of Justice., (1986) Military and Paramilitary Activities in and against Nicaragua (Nicaragua*

ISSN: 2582-6433

decade, American tort law has begun to adapt to cover online harms such as Internet defamation, email stalking, spamming, and trespassing on websites[10].

III. CYBER WRONG AND ITS TYPE

Cyber wrongs are unauthorized acts that are committed over the internet. The wrong is mainly done by the involvement of technology. Cyber wrongs encompass both civil and criminal wrongs. The Information Technology Act imposes civil and criminal fines for violations of its provisions.

1. **A civil cyber wrong** is committed online and is civil in nature, such as a tort of defamation committed online using a computer (or any device with internet access and the ability to modify or post information online, such as a mobile phone or a tablet) as a tool to commit that type of wrong. Although not specified or treated as civil cyber wrongs, section 43 of the IT Act of 2000[11] defines the essence of civil liability. A civil proceeding occurs when one person or state seeks to assert their civil rights against another person. If the claim is successful, it will result in the declaration of the claimed rights and relief. If a court order is directed against a criminal act, it must be considered criminal if it could result in imprisonment or a fine. Civil Sanctions aim to protect the harmed parties and make the violation justifiable.
2. **A criminal cyber wrong** is a major problem that must be addressed as quickly as feasible. A criminal cyber wrong is a crime committed online using technology, including hacking, information theft, denial of service attacks, and so on. Although not treated as criminal cyber wrongs in any acts, many wrongs of a criminal nature are defined under the IT Act of 2000[12], such as child pornography under Section 67-A of the act. A criminal punishment is a prosecution resulting in a fine or imprisonment under a statute. It is based on the notion that society suffers as a result of the defaulter's actions and that a deterrent sentence is necessary to prevent the infraction from occurring again. The proceedings for damages are independent from the criminal accusations brought against the offender. The imposition of damages does not constitute a prosecution or punishment for any offense. It can be done simultaneously with filing a criminal complaint.

Civil sanctions defend a person's property or privacy rights, while criminal sanctions aim to

v. United States of America).

[10] The article named; Cyber Torts written in ennstate is referred for the introduction part of the project; i.e. The basic idea of Cyber Tort.

[11] IT Act 2000.

[12] New Amendments to IT Act 2000.

ISSN: 2582-6433

uphold public justice by punishing offenders. Thus, the two therapies are mutually exclusive, although they clearly coexist and fundamentally differ in their content and outcome.

IV. IMPACT OF TECHNOLOGY IN THE WORLD

Over the years, technology has transformed our world, creating incredible tools and resources that put extremely useful knowledge at the fingertips of every person. The digital revolution has been both a blessing and a curse, as e-filing in courtrooms has become a regular occurrence, and information about cases is now being posted online on websites, as well as a curse because some of the wrongs that were previously possible in the real world, such as digital defamation, cyberstalking, and so on, are now also possible in the virtual world[13].

E-governance has made it much easier for the Indian government to provide government services, communicate information, and so on, resulting in a reduction in paper usage and a promotion of the technical sector. It is now easy to obtain everything online rather than through paper and files[14].

V. TORT CONCEPT IN THE CYBERWORLD

As previously stated, a tort is a negligent or intentional act that is done by someone who injures someone else in some way, either physically or by violating their legal rights[15]. Cyber torts, which are committed over cyberspace, are very important because they are on the rise and can have serious repercussions on society. Everyone in society should be aware of the dangers and damage that is caused by cyber torts because technology has become an essential part of life for everyone. Examples of cyber torts include e-mail harassment, cyberstalking or cyber harassment, and cyber defamation[16].

1. Cyber Stalking

Stalking has long been recognized as an unwelcome behavior of an obsessive stalker towards a distressed victim. Although this concept has existed for a long time, its influence has just recently emerged. Cyberstalking is the use of information and communication technologies to harass, distress, and instil fear in others.

---

[13] *C. Scheideler, "Theory of network communication", Johns Hopkins University, September 2002.*
[14] *Vakul Sharma, Information Technology: Law and Practice, Universal Law Publishing Co. Pvt.Ltd., 2008.*
[15] *Cyberspace available at: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_ Lander, A Filipino Linked to "Love Bug" Talks About His License to Hack, N.Y. TIMES, October 21, 2000.*
[16] *Adv. Prashant Mali, "Types of cyber-crimes & cyber law in India", CSI Communication, Vol. 35, issue 8, pp. 33-34, November 2011.*

ISSN: 2582-6433

Cyber stalkers use internet services like e-mails to send threatening, disturbing, and harassing communications to victims. Stalking can be done directly or indirectly. In direct harassment, the stalker delivers harassing messages to the victim directly, whereas indirect harassment involves obtaining personal information and using it to contact the individual through other ways.

Cyberstalking creates a danger to many internet users, who cannot simply move away or disconnect from the internet. Stalking in cyberspace does not leave direct viewing traces, requires digitalized effects, and may only be detected by computerized means. However, it harms the victim who lives in reality[17].

2. Cyber Harassment

Harassment via email is not a new concept. It is very similar to harassment by letter. Recently, I received an email from a lady who complained about the same. Her previous boy friend was continually sending her emails, sometimes emotionally blackmailing her and threatening her. This is a common kind of email harassment.

3. Cyber Defamation

It is the act of imputing any individual with the intent to reduce the person's standing in the eyes of right-thinking members of society as a whole, to cause him to be shunned or avoided, or to expose him to hatred, scorn, or ridicule. Cyber defamation is identical to traditional defamation except for the use of a virtual medium. For example, Rohit's email account was hacked, and emails were sent from his account to some of his batch mates about his affair with a female to discredit him.

4. Hacking

This action is often known as hacking. The Indian law has given a different sense to the term hacking, thus we will not use the term "unauthorized access" interchangeably with the term "hacking" to avoid confusion, as the term employed in the Act of 2000 is far broader than hacking[18].

5. Cyber-Vandalism

Conventional vandalism refers to the wilful destruction or damage of someone's property. Thus,

[17] *Cyber tort available at: www.cyberessays.com/lists/cyber-torts//last visited on 25th Mar 2024.*
[18] *Cyber tort available at: www.legalservicesindia.com/article/1134/Cyber-Torts.html last visited on 29th Mar 2024.*

ISSN: 2582-6433

cyber-vandalism refers to intentionally causing physical harm to anyone's computer or virtual system. These activities may include the theft of a computer or any of its peripherals[19].

6. Cyber Trafficking

Trafficking can take various forms, including drugs, weaponry, and even human beings. Trafficking has taken on a new form with the rise of the internet, as cyber trafficking has emerged, in which the trafficking procedure is carried out online via a virtual machine.

7. Cyber Obscenity

Pornography on the internet takes numerous forms. It may also feature banned content, like as child pornography, which is a serious felony in real life.

8. Intellectual Property Crimes

Intellectual property consists of a set of rights. Any unlawful conduct that deprives the owner of his rights, whether entirely or partially, is an offense. Software piracy, copyright infringement, trademark and service mark violations, theft of computer source code, and so on are examples of prevalent IPR violations. In a landmark decision, the Hyderabad Court convicted three people and sentenced them to six months in prison and 50,000.

VI. MANNER OF COMMITTING TORT.

1. Theft Of Information Contained in Electronic Form

This comprises information stored on computer hard disks, removable storage media, magnetic disks, flash memory devices, and so on. Theft can occur either by physically stealing or misappropriating data or by meddling with it via the virtual medium.

Example- When a person receives random emails including links to a replica of any website that requires personal information to log in, filling out the form provides the user who built the replica with all of the victim's information and access to the account.

2. E-mail Bombing

This type of action relates to sending massive amounts of mail to the target, which could be an

[19]*Cyber awareness available at: www.researchgate.net/publication/267470949_Cyber_Situational_Awareness_Issues_and_Research last visited on 30th Mar 2024.*

ISSN: 2582-6433

individual, a company, or even mail servers, ultimately resulting in crashing.

3. **Trojan Attack**

Also known as Trojan horses, these are the types of software that are installed on a computer by masquerading as authorized software while not being authentic. This software acquires administrative access to computers passively, without informing the actual owner.

4. **Chat Rooms and Message Boards**

Chat rooms and Message boards can lead to cyberstalking.

Example- Certain groups of people build websites that target people suffering from mental illness or despair, convincing them that there is no chance for them to continue living their lives through message boards or chat rooms.

5. **Data Dwindling**

These attacks involve modifying raw data before a computer operation is completed and then restoring the information to its prior state.

6. **Virus**

These are the programs that attach themselves to a computer and begin multiplying to cease filling the computer's data after getting administrative access to the machine.

7. **Denial of Service Attack**

In this mode, a server is inundated with requests, which may cause the server to crash and prevent the site from functioning.

8. **Web Jacking**

This phrase is derived from the term hi-jacking. In these types of offenses, the hacker acquires access to and control of another person's website. He may even mutilate or alter the information on the website. This may be done to achieve political goals or to make money. For example, recently, the Ministry of Information Technology site was found hacked by Pakistani hackers, and some obscenity was found posted there. The Bombay Crime Branch's website was also hacked[20]. Another example of web hacking is the classic Fish Case. In this situation, the site was

[20] *Lander, A Filipino Linked to "Love Bug" Talks About His License to Hack, N.Y. TIMES, October 21, 2000.*

ISSN: 2582-6433

hacked, and the information related to the goldfish had transformed. Furthermore, a ransom of US$1 million was demanded. Thus, web jacking is a method in which control over another's site is obtained in exchange for some consideration[21].

VII. PEOPLE WHO MAINLY COMMIT CYBERCRIME

1. People Between the Ages Of 6 To 16

People of this age range are not intellectually evolved enough to understand the consequences of the actions they may take; therefore, cyber wrongs perpetrated by these folks are sometimes committed without even realizing it. The offenders are called Juveniles.

2. People Who Are Unaware of Cyber Wrongs

There is still a large group of people in India who are unaware of the wrongs that they may end up committing online without realizing the consequences of their actions or the penalties of the offenses that they may commit. Typically, people in underdeveloped countries may commit these wrongs because there are no proper rules and regulations in place. After all, technology is still a relatively new term in these countries.

3. Professional Hackers

Independent hackers are typically held liable for all types of cybercrimes done online.
Example - Individual hackers who are not linked with any organization are paid by individuals to carry out a specific mission online against another individual.

4. Organised Hackers

Certain organizations are founded by hackers with the sole purpose of achieving political prejudice, fundamentalism, or other similar objectives.
Example - Organizational hackers recruited informally by political parties to work online and post things against their opponents that a person would ordinarily not do, or even hack their official website and change the full of it.

5. Terrorist Attack

Terrorist organizations play an important role in the world of cybercrime because they are

[21] *Cyber tort and cyberspace available at: www.researchgate.net/publication/344507432_Cyber_Attack_Cyber_Tort_and_Cyber_Security last visited on 31st Mar 2024.*

ISSN: 2582-6433

responsible for motivating and hiring youth into their organizations to carry out their agendas. This is accomplished by using social media as a medium to connect with potential individuals, and thus they are manipulated over the internet to carry out specific acts that may be against an individual or the state.

VIII. LEGAL FRAMEWORK

To address the issues that arise in the cyber world, the Information Technology Act was passed in 2000.

The primary goal of this act was to establish legal recognition for electronic records with the government. India has several well-codified laws that are still applicable today; yet, the rise of the internet has brought with it new legal challenges.

Existing laws were enacted in the past with society, politics, economics, and culture in mind. There was no internet in the past, thus there was no need for cyber laws; however, this is no longer the case, as we have entered the cyber era and must deal with legal concerns concerning the internet and the cyber world[22].

The laws that existed in India could not be construed in the context of the offense committed online, therefore there was a need for the formulation and enactment of cyber laws, as none of the existing laws provided legal validity to cyber activities.

According to section 1(2), the act applies to all of India and also to any offense or contravention committed by someone outside of Indian territory, as stated in section 75 of the act. However, without a written extradition treaty arrangement, a trial for such wrongs is extremely hard.

The statute was created to address all cybercrimes that may occur on the internet.

The Act was updated in 2008, and the establishment of cyber appellate tribunals was outlined in Section 48 of the Act. The tribunal was established to deal with all cyber-related issues in India, and it has the same powers as a civil court.

The 2008 amendment made various changes to the act, such as clarifying the word "communication devices" and holding firms accountable for security breaches caused by poor data security practice implementation.

IX. CONCLUSION

No government in the world can prevent cybercrime or other internet wrongs committed by people regularly. However, governments may adapt and expand their technologies while

[22] *Available at: blog.ipleaders.in/cyber-torts// last visited on 30th Mar 2024.*

ISSN: 2582-6433

monitoring everyone's online actions in cyberspace.

Historically, no legislation in any world has been able to abolish the wrong against which it was enacted. The same is true for India's cyber laws; as the cyber world expands, new ways to exploit gaps on the internet and conduct wrongs emerge daily.

Because many individuals are uninformed of the wrongs that can occur online and the penalties associated with them, the government should adopt a strategy to publicize the crimes and the penalties associated with them so that even the average person can be informed of the consequences of such activities.

Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of

International Information Security, 61st plenary meeting (Dec. 2, 2008) [hereinafter Shanghai Cooperation Agreement]

Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of

International Information Security, 61st plenary meeting (Dec. 2, 2008) [hereinafter Shanghai Cooperation Agreement]

Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of

International Information Security, 61st plenary meeting (Dec. 2, 2008) [hereinafter Shanghai Cooperation Agreement]

Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of

International Information Security, 61st plenary meeting (Dec. 2, 2008) [hereinafter Shanghai Cooperation Agreement]

Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, 61st plenary meeting (Dec. 2, 2008) [hereinafter Shanghai Cooperation Agreement]

Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, 61st plenary meeting (Dec. 2, 2008) [hereinafter Shanghai Cooperation Agreement].

2.http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspa c e.pdf.. Mark Lander, A Filipino Linked to “Love Bug” Talks About His License to Hack, N.Y.

ISSN: 2582-6433

TIMES, October 21, 2000

3. Article named Cyber Tort in the famous American Journal of International Commercial Law and Technology written by 'Gregory C.

Mosier' and 'Tara' has been utilized to get the matter on types of cyber Torts in India.

4. International Court of Justice., (1986) Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of

America).

5. Article named, Cyber Torts written in ennstate is referred for the introduction part of the proect; i.e. The basic idea of Cyber Tort.

6. Vakul Sharma, Information Technology: Law and Practice, Universal Law Publishing Co. Pvt.

Ltd., 2008.

7. IT act 2000

8. New Amendments to IT Act 2000

9. S. Hinde, "The law, cybercrime, risk assessment and cyber protection", Computers & Security, vol. 22, issue 2, pp. 90-95, February 2003.

10. C. Scheideler, "Theory of network communication", Johns Hopkins University, September 2002.

11. Adv. Prashant Mali, "Types of cyber crimes & cyber law in India", CSI Communication, Vol. 35,

issue 8, pp. 33-34, November 2011.

12. Q. Yeh and A. Chang, "Threats and countermeasures for information system security: A cross-

industry study", Information & Management, vol. 44, pp. 480-491,