ANALYTICAL AND COMPARATIVE APPROACH OF LAWS IN CYBER SPACE (A GEOGRAPHICAL SPECTRUM)

Shweta Chaku[1], Amrita Bhatnagar[2], Kamna Singh[3]

[1,2,3]*CSE, Inderprastha Engineering College/ UP University, (India)*

ABSTRACT

This paper explores the various laws used to deal different socio-economic attacks under different jurisdiction. Cyber attacks may have some motivation behind it or may be processed unknowingly. The attacks those are processed knowingly can be considered as the cyber crime and they have serious impacts over the society in the form of economical disrupt, psychological disorder, threat to National defense etc. Restriction of cyber crimes is dependent on proper analysis of their behavior and understanding of their impacts over various levels of society. Therefore, the current manuscript provides the understanding of cyber crimes and their impacts over society with the future trends of cyber crimes.

Keywords: Cyber Attacks, Cyber Crimes, Consumer trust, Stalking, National Security

I. INTRODUCTION

Cyber-attack is a kind of repulsive and offensive behavior implemented by individuals or whole organizations. The main objective is to aim at computer information systems, infrastructures, computer networks, and/or personal computer by actions of crackers.tha action can be performed with the aim of stealing, altering, or destroying a specified target by hacking into a susceptible system. Cyber-attacks can range from installing spyware on a PC to attempts to destroy the infrastructure of entire nations.

II. IMPACT ON VARIOUS SOCIAL SECTORS

2.1 Impact Against Government

There are certain offences done by group of persons intending to threaten the international governments by using internet facilities. It includes:

Cyber Terrorism: Cyber terrorism activities endanger the sovereignty and integrity of the nation.

Distribution of pirated software: It means distributing pirated software from one computer to another intending to destroy the data and official records of the government.

Possession of Unauthorized Information: It is very easy to access any information by the terrorists with the aid of internet and to possess that information for political, religious, social, ideological objectives.

2.2 Impact Against Society

An unlawful act done with the intention of causing harm to the cyberspace will affect large number of persons. These offences include:

Cyber Stalking/Online harassment: When a victim is repeatedly and persistently followed and pursued online by e-mail or other electronic communication by offenders.

Online Child Pornography: Online child pornography is defined by pedophiles using computer resources to distribute illegal media of and to minors, as well as engaging in actions to sexually exploit children.

Cyber Bullying: Acts of harassment, embarrassment, threatening behavior towards a victim by using internet, e-mail or other electronic communication device.

Cyber Warfare: conducting sabotage and espionage.

Hacking: It is an electronic intrusion, or gaining access to resources like computer, e-mail or social networking accounts such as Face book, Orkut, Gmail, and Hotmail etc. via a computer or network resource without permission.

Unwanted exposure to sexually explicit material etc.: When a criminal sends pictures, videos, sound clips, cartoons or animations depicting sexual contents by e-mail or any other electronic means. This would include audio or video chat using web camera etc.

2.3 Impact on Bussiness

As all the businesses, all over the world are increasingly operating in the online mode because most of their work being done through websites, hence all sectors are equally vulnerable to cyber crime. Cyber Crimes always affects the companies

Identity Theft: When someone appropriates another's personal information without his or her knowledge to commit theft or fraud. Identity theft is a vehicle for perpetrating other types of fraud schemes. Typically, the victim is led to believe they are divulging sensitive personal information to a legitimate business, sometimes as a response to an e-mail solicitation to update billing or membership information, or as an application to a fraudulent Internet job posting.

Malicious Programs/Viruses: Viruses and malicious programs can potentially impact a massive amount of individuals and resources. These programs are intended to cause electronic resources to function abnormally and may impact legitimate users access to computer resources.

Spam: It is the distribution of bulk e-mail that offers recipients deals on products or services. The purpose of these unsolicited mails is to make customers think they are going to receive the real product or service at a reduced price. However, before the deal can occur, the sender of the spam asks for money, the recipients‟ credit card number or other personal information. The customer will send that information and never receive the product nor hear from the spammer.

Spoofing: It is a technique whereby a fraudster pretends to be someone else's email or web site. This is typically done by copying the web content of a legitimate web site to the fraudster's newly created fraudulent web site.

Phishing: Phishing refers to the scheme whereby the perpetrators use the spoofed web sites in an attempt to dope the victim into divulging sensitive information, such as passwords, credit card and bank account numbers. The victim, usually via email is provided with a hyperlink that directs hi/her to a fraudster's web site. This fraudulent web site's name closely resembles the true name of the legitimate business.

Denial of Service: A denial of service attack is a targeted effort to disrupt a legitimate user of a Service from having access to the service. Offenders can limit or prevent access to services by overloading the available resources, changing the configuration of the service's data, or physically destroying the available connections to the information

Computer Fraud: It is one of the most rapidly increasing forms of computer crime. It is also commonly referred to as Internet fraud. Essentially, computer or Internet fraud is "any type of fraud scheme that uses one or more components of the Internet-such as chat rooms, e-mail, message boards, or Web sites to present fraudulent transactions or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme"

III. ENFORCING CYBER LAWS: AN URGENT AND UPDATED NEED

There is a need to adopt a strict law by the cyber space authority to regulate criminal activities relating to cyber and to provide better administration of justice to the victim of cyber crime. In the modern cyber technology world it is very much necessary to regulate cyber crimes and most importantly cyber law should be made stricter in the case of cyber terrorism and hackers. Mostly peoples don't know about cyber crime/cyber laws. so today's need to aware the society

3.1 Implementation of Laws Defined for Each Jurisdiction

3.1.1 Cybercrime Laws of the United States

Substantive cybercrime laws (e.g., laws prohibiting online identity theft, hacking, intrusion into computer systems, child pornography, intellectual property, online gambling):

- Fraud and related activity in connection with identification documents, authentication features, and information 18 U.S.C. § 1028
- Aggravated identity theft 18 U.S.C. § 1028A
- Fraud and related activity in connection with access devices 18 U.S.C. § 102
- Fraud and related activity in connection with computers 18 U.S.C. § 1030
- Fraud and related activity in connection with electronic mail 18 U.S.C. § 1037
- Fraud by wire, radio, or television18 U.S.C. § 1343
- [Malicious mischief related to] Communications lines, stations, or systems 18 U.S.C. § 1362
- Importation or transportation of obscene matters 18 U.S.C. § 1462
- Transportation of obscene matters for sale or distribution 18 U.S.C. § 1465
- Obscene visual representation of the sexual abuse of children 18 U.S.C. § 1466A
- Sexual exploitation of children 18 U.S.C. § 2251
- Certain activities relating to material involving the sexual exploitation of minors 18 U.S.C. § 2
- Certain activities relating to material constituting or containing child pornography 18 U.S.C. § 2252A
- Misleading domain names on the Internet [to deceive minors] 18 U.S.C. § 2252B
- Misleading words or digital images on the Internet 18 U.S.C. § 2252C
- Use of interstate facilities to transmit information about a minor 18 U.S.C. § 2425
- Criminal infringement of a copyright 18 U.S.C. § 2319
- Criminal offenses [related to copyright] 17 U.S.C. § 506
- Unauthorized publication or use of communications The Unlawful Internet Gambling Enforcement Act of 2006 Procedural cybercrime laws (e.g., authority to preserve and obtain electronic data from third parties, including internet service providers; authority to intercept electronic communications; authority to search and seize electronic evidence): 47 U.S.C. 605
- Interception of wire, oral, or electronic communication 18 U.S.C. §§ 2510-2522

- Preservation and disclosure of stored wire and electronic communication 18 U.S.C. §§ 2701-2712
- Pen registers and trap and trace devices Computer Crime and Intellectual Property Section18 U.S.C. §§ 3121-3127

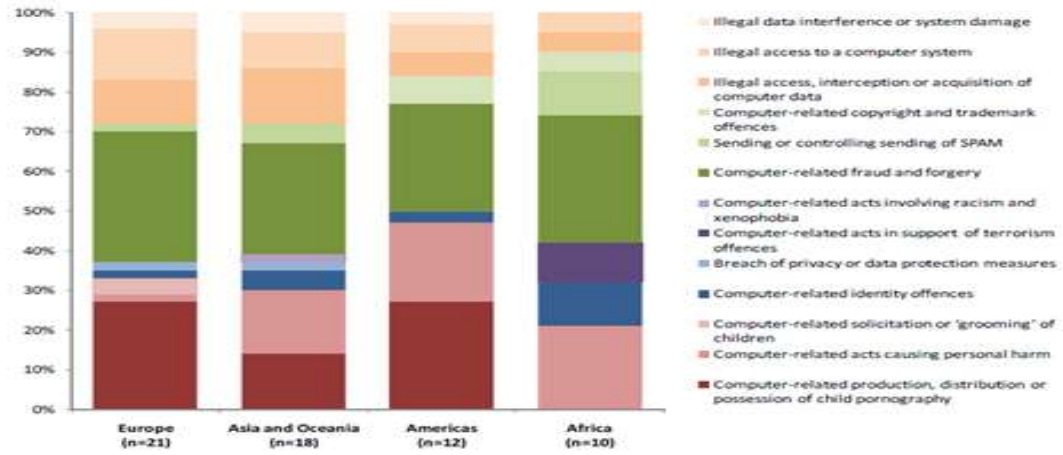
Fraud and related activity in connection with identification documents, authentication features, and information (a) Whoever, in a circumstance described in subsection (c) of this section— (1) knowingly and without lawful authority produces an identification document, authentication18 U.S.C. § 1028

3.1.2 Cyber Law in India

Offences under IT Act

- Tampering with computer source Documents Sec.65
- Hacking with computer systems , Data Alteration Sec.66
- 3. Sending offensive messages through communication service, etc Sec.66A
- Dishonestly receiving stolen computer resource or communication device Sec.66B
- Identity theft Sec.66C
- Cheating by personating by using computer resource Sec.66D
- Violation of privacy Sec.66E
- Cyber terrorism Sec.66F
- Publishing or transmitting obscene material in electronic form Sec .67
- Publishing or transmitting of material containing sexually explicit act, etc. electronic form Sec.67A
- Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form Sec.67B
- Preservation and Retention of information by intermediaries Sec.67C
- Powers to issue directions for interception or monitoring or decryption of any information through any computer resource Sec.69
- Power to issue directions for blocking for public access of any information through any computer resource Sec.69A
- Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security Sec.69B
- Un-authorized access to protected system Sec.70
- Penalty for misrepresentation Sec.71
- Breach of confidentiality and privacy Sec.72
- Publishing False digital signature certificates Sec.73
- Publication for fraudulent purpose Sec.74
- Act to apply for offence or contraventions committed outside India Sec.75
- Compensation, penalties or confiscation not to interfere with other Punishment Sec.77
- Compounding of Offences Sec.77A
- Offences with three years imprisonment to be cognizable Sec.77B
- Exemption from liability of intermediary in certain cases Sec.79
- Punishment for abetment of offences Sec.84B
- Punishment for attempt to commit offences Sec.84C
- Offences by Companies Sec.85

- Sending threatening messages by e-mail Sec .503 IPC
- Word, gesture or act intended to insult the modesty of a woman Sec.509 IPC
- Sending defamatory messages by e-mail Sec .499 IPC
- Bogus websites ,Cyber Frauds Sec .420 IPC
- E-mail Spoofing Sec .463 IPC
- Making a false document Sec.464 IPC
- Forgery for purpose of cheating Sec.468 IPC
- Forgery for purpose of harming reputation Sec.469 IPC
- Web-Jacking Sec .383 IPC
- E-mail Abuse Sec .500 IPC
- Punishment for criminal intimidation Sec.506 IPC
- Criminal intimidation by an anonymous communication Sec.507 IPC
- When copyright infringed:- Copyright in a work shall be deemed to be infringed Sec.51
- Offence of infringement of copyright or other rights conferred by this Act.Any person who knowingly infringes or abets the infringement of Sec.63
- Enhanced penalty on second and subsequent convictions Sec.63A
- Knowing use of infringing copy of computer programmers to be an offence Sec.63B
- Obscenity Sec. 292 IPC
- Printing etc. of grossly indecent or scurrilous matter or matter intended for blackmailSec.292A IPC
- Sale, etc., of obscene objects to young person Sec .293 IPC
- Obscene acts and songs Sec.294 IPC
- Theft of Computer Hardware Sec. 378
- Punishment for theft Sec.379
- Online Sale of Drugs NDPS Act
- Online Sale of Arms Arms Act



IV. CONCLUSION

When assessing the effect of cybercrime, it's necessary to evaluate a series of factors: The loss of intellectual property and sensitive data, Opportunity costs, including service and employment disruptions, damage to the brand image and company reputation. Penalties and compensatory payments to customers (for inconvenience or

consequential loss), or contractual compensation (for delays, etc.) Cost of countermeasures and insurance. Cost of mitigation strategies and recovery from cyber attacks, loss of trade and competitiveness, distortion of trade and job loss. Amendments have been proposed and laws are updated. Changes in the Amendment include: redefining terms such as "communication device" to reflect current use; validating electronic signatures and contracts; Making the owner of a given IP address responsible for content accessed or distributed through it; and making corporations responsible for implementing effective data security practices and liable for breaches.

The Amendment has been criticized for decreasing the penalties for some cybercrimes and for lacking sufficient safeguards to protect the civil rights of individuals.

REFERENCES

[1]. http://www.rpost.com/esigning/benefits
[2]. http://en.wikipedia.org/wiki/Digital_signature
[3]. http://www.arx.com/digital-signatures-faq
[4]. http://www.youdzone.com/signature.html
[5]. http://www.lawzonline.com/bareacts/information-technology-act/information-technology-act.html
[6]. http://www.instantssl.com/https-tutorials/digital-signature.html
[7]. http://www.youdzone.com/signature.html
[8]. http://www.nasscom.in/vision-and-mission
[9]. http://mpcyberpolice.nic.in/pdf/7.pdf