JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Juridical Study on New Directions in Cybercrime

DETAILS OF AUTHOR & CO-AUTHOR

Name of Author : Barnali Deka
Designation : Assistant Professor
University : University School of Law and Research, USTM
Phone No : 9707919384
Email Id : barnali.js.22@gmail.com

Name Co-author : Marphy Hiloidhary
Designation : Assistant Professor
University : University School of Law and Research, USTM.
Phone No : 8472921879
Email id : hiloidharychetia1990@gmail.com

Abstract: The 21st century has been characterized by massive technological innovations that have shaped the way people interact and communicate with the surrounding. The social, political, and economic dimensions of human life are facilitated by a digital age that has encompassed the whole world. Universally, there has been a rapid rise in the use of computers and electronic gadgets. These developments have led to significant growth in criminality, especially in cyberspace. Cybercrimes have grown progressively with perpetrators developing newer and sophisticated techniques every day. Despite the measures taken by the international community to combat the vice and mitigate its effects, cybercrimes have continued to rise alarmingly across the world. The aim of the research is to examine the negative impact cybercrimes pose to the society by doctrine research based on secondary sources of data such as books, journal, magazine, newspaper, reports & internet. Cyber crime is said to be of those species of which genus is the conventional crime and where either the computer is an object or subject of the conduct constituting crime.

Keywords: Cybercrime, Computer Crime, Hacktivism, Cyber Pornography, Stalking etc.

Introduction

With the development of information technology and electronic devices successful communication through the internet, thriving businesses and global interaction through social media platforms has increased. The world has entered the digital age where technology is ever-present and all persistent.[1] The development of technological innovations facilitates our day to day lives

*****Assistant Professor, University School of Law & Research, USTM
****** Assistant Professor, University School of Law & Research, USTM

[1] Cyber-dependent criminality was acutely felt across the world in May 2015 when Cryptowall 3.0 ransomware began attacking businesses. Using an exploit kit capable of attacking software vulnerabilities, Cryptowall 3.0 searched for files on the victims computers encrypted these documents, deleted the originals and then alerted the victims that they needed to pay thousands of

and working schedule with comfort and fastest means. However, with that growth of technology, it also creates noteworthy contributions to criminality. Cybercrime has become a serious problem globally where the research need to match the reality which is struggling to keep up with the moving pace. There is a need for more academics curriculum to get involved in cybercrime prevention and cyber security research inviting interdisciplinary research too. The work needs not only a criminological lens, but a massive amount of lenses in order to understand the impact of cybercrime across the globe. Since half of all internet users are located in Asia there is an urging need to encourage academics to do cyber security and cybercrime research in the Asia-Pacific region. However, these developments are threatened by criminal activities in the world's cyberspace. Computer crime has become a major global challenge and continues to be a major concern for international security. With the advent of rapid internet and new technology, cybercriminals have the chance to infiltrate individuals and businesses via their computer systems.[2]. Every day, there are new developments in malicious software and viruses that are developed across the world. Around million of people are exaggerated by compromised computer systems every day where cybercrime has led to significant damages not only for individuals but also for businesses whereby it causes employment disruptions and reduced trust for a company's online activities.[3]

Violation of data refers to unlawful gaining of information by unauthorized persons that often compromises security or integrity and personal information.[4] Cybercriminals all over the world can only be brought to justice if there are available and ample laws to combat the vice. Further, there is a need to connect in proactive strategies while observing cybercrime attacks. As the internet came into widespread commercial use the life of computer crimes began to shift. 'While in some crimes one component of the crime may have been committed using an electronic instrument, in other crimes, the crime as whole is committed in the online or electronic environment. These crimes, known as cybercrimes, generally occur in the virtual community of the internet or in cyberspace.' Viruses, worms, and Trojan horses are certain serious mode of threat.[5] There is a variety of cyber crime committed but these are the most prevalent and appear to be among the most troubling to computer users.Cyber-dependent crimes are those crimes that cannot exist without the cyber technology. A cybercriminal can inflict massive commercial damage by using the internet and by assessing it with all its illegal activities. In fact, it is now easier and safer for a criminal to disrupt a business by destroying its database through malware than by throwing a Molotov cocktail through its front door.

History of Cyber Crime

The first Cyber Crime was recorded within the year 1820. The primeval type of computer has been in Japan, China and India since 3500 B.C, but Charles Babbage's analytical engine is considered as the time of present day computers. The device authorized a series of steps that was continual within the weaving of special fabrics or materials. This resulted in an exceeding concern amongst the Jacquard's workers as their livelihoods and their traditional employment were threatened as it preferred to interrupt to discourage Jacquard so that the new technology cannot be utilized in the future.[6]

Society and Cyber Crime

Cyber crime and society provides a systematic, clear and a serious analysis of the recent debates about cybercrime in various aspects of life. It trace the phenomenon in its wider contexts of social, political, cultural, and economic changes.[7] The world of technology has become parallel form of lives in the most easiest means. It has been emerging as the serious threat as the government, police departments and intelligence units have started to react upon the massive destruction caused by cyber crime to the society. So as various legal measures are endured for its remedial measures to ensure peace and security in work lives with

---

dollars in ransom money in order to get their files back. It has been recorded that these attacks tainted hundreds of thousands of computers around the world causing close million damage.

[2] For example, Interpol reports clarify that there are millions of cases that attempt to illegally access and interfere with other people's files

[3] It is estimated that the damages worldwide accrue to over 2.8 billion dollars every year. Data breaches have become a norm for big social media companies such asFacebook and TikTok.

[4] The US senate committee in 2020 released reports screening that a Chinese firm led to breach of privacy regulations as it's a database consisting of customer records that was shared with third parties. However the responsibilities ofcommunicating cybercrime activities lie in individual countries which should ensure that they protect and empower institutions to create an organized mitigation campaign that monitors what happens in cyberspace.

[5]A.I.R 2006 SC 2820; Paranjape N.V(Dr), Criminology and Penology,13th edition, 2019

[6] Introduction to Cyber Crimes available at https://www.subhartidde. com/slms/Cyber% 20Crime%20 and%20 Law% 20(BBA-103).pdf, retrieved on 12th December, 2021

[7]www.researchgate.net

complete encrypted procedures.[8] As the use of internet came into a widespread commercial use, the nature of computer crimes too being to be shifted as in some crimes one of the component have been committed by using electronic instrument while in others the crime is committed as a whole in the online or electronic environment[9].

Classifications of Cyber Crime

Cyber Crime can be classified into four major categories. They are as follows:

a) Cyber crime against individuals:[10] Crimes that are committed by the cyber criminals against an individual or a person. A few cybercrime against individuals are:

- **Email bluffing**: This method is a forgery of an email header. This means that the message appears to have received from someone or somewhere other than the genuine or actual source. These strategies are usually used in spam campaigns or in phishing, because people are probably going to open an electronic mail or an email when they think that the email has been sent by a legitimate source.
- **Spamming**: Email spam which is otherwise called as junk email. It is unsought mass message sent through email, where the uses of spam have become popular in the mid 1990s and it is a challenging issues faced by most email users now a days. Recipient's email addresses are obtained by spam bots, which are automated plans that skulks the internet in search of email addresses. The spammers use spam bots to create email distribution lists. With the expectation of receiving a few number of respond a spammer naturally sends an email to millions of email addresses.
- **Cyber defamation**: Cyber defamation means the harm that is brought on the reputation of an individual in the eyes of other individual through the cyber space. The purpose of making defamatory statement is to bring down the reputation of the individual.
- **Internet Relay Chat:**[11] IRC servers allow the people around the world to come together under a single platform which is sometime called as rooms and they chat to each other.[12]
- **Phishing**: In this type of crimes or fraud the attackers tries to gain data such as login information or account's information by masquerading as a reputable individual or entity in various messages channels or in email.

b) Cyber Crime against property: These sorts of crimes includes vandalism of computers, Intellectual Property Crimes, Online threatening etc. Intellectual property crime includes:

- **Software piracy**: It is define as the copying of software unauthorizedly.
- **Copyright infringement**: It can be described as the infringements of an individual or organization's copyright. In simple term it can also be describes as the using of copyright materials unauthorizedly such as music, software, text etc.
- **Trademark infringement**: It can be described as the using of a service mark or trademark unauthorizedly.

c) Cyber crime against organization: Cyber Crimes against association are as follows:

- Unauthorized changing or deleting of data.
- Analysis or photocopying of confidential data unauthorizedly but the data are neither being change nor deleted.
- **DOS attack**: In this attack, the attacker floods the servers, systems or networks with traffic in order to overwhelm the victim resources and make it impracticable or difficult for the users to use them.
- **Email bombing**:

  It is a sort of Net Abuse, where huge numbers of emails are sent to an email address in order to excess or flood the mailbox with mails or to flood the server where the email address is.

[8]http://citeseex.ist.psu.edu
[9]http://www.ajol.info.com
[10] Net extortion, Hacking, Indecent exposure, Trafficking, Distribution, Posting, Credit Card, Malicious code etc. The latent harm of such a malefaction to an individual person can hardly be bigger.
[11] Factors behind IRC to combat the menace of crimes are - Chat to win ones confidence and later starts to harass sexually, and then blackmail people for ransom, and if the victim denied paying the amount, criminal starts intimidating to upload victim's nude photographs or video on the internet; A few are paedophiles they harass offspring for their own benefits; A few uses IRC by offering fake jobs and sometime fake lottery and earns money.
[12] Cyber offenders basically uses it for meeting; Hacker uses it for discussing their practices; Paedophiles use it to allure minors.

d) Cyber crime against society: Cyber Crime against society includes-

- **Forgery**: Forgery means making of false document, signature, currency, revenue stamp etc.
- **Web jacking**: The term "Web jacking" has been derived from hi jacking. In this offence the attacker creates a fake website and when the victim opens the link a new page appears with the message and they need to click another link. If the victim clicks the link that looks real he will redirected to a fake page. These types of attacks are done to get entry or to get access and controls the site of another. The attacker may also change the information of the victim's webpage .
- **Cyber-pornography:** Cyber-pornography mentions expressly to progeny pornography on the internet usually engaging those less than 18 years of age. While enclosures in the United States and Europe have discovered mature individual pornography on the internet to drop lawful boundaries .There is an efficiently agreed lawful, psychological and communal agreement that young children are not to be engaged in the international sex industry.[13]

Impact of Cyber Crime over Teenager & Youth:

These days a worst terror in teenager's eyes is Cyber Bullying.[14] It is a common over past five years generally from the age below eighteen they are more prone from Cyber Bullying as per inspection. It is an alarming trend in our society as per the inspection of data, the worst fear of cyber crime is female teenagers. Cyber Bullying is when person receives threats, negative comments or negative pictures or comments from other person.

Cyber communication is one of the society's modern way to communicate. Online social networking websites, text messages and emails provide users with an effective quick way to communicate with people all over the world. Teens in particular spend hours after hours every day on computers or personal electronic devices. The use of social networking sites has increasingly become popular among youths as it enables to stay connected to real and online friends. Some teens believe cyber connections help them feel confident to be their true selves. Instant messaging programs, used by projected 13 million teens, allow conversations with friends to occur in real time. An online communication tool opens the door for friendships with other teens near and far is an ongoing process. Sexual solicitation is a growing concern for adolescence that uses forms of cyber communication. It may occur in chat rooms or on social networking sites. Sexual solicitation occurs where an adult or peer tries to engage in an online sexual relationship. A teen may be asked to disclose personal information view pornography or discuss something sexual online. About 70 percent of teens who are sexually solicited online are girls. Teens should be careful in posting suggestive photos online and talking to strangers in chat rooms.

Safety in cyberspace:

Some points that one should keep in mind while surfing the internet. If possible always use a strong password and enable two steps or two-step authentication[15] in the webmail. It is very important in order to make webmail or social media account secured. Following are the few guidelines of strong password-

1. Password should be of minimum eight characters.
2. One or more than one of lower case letter, upper case letter, number, and symbol should be included.

[13] Leon Radzinovicz, The Growth of Crime, p 202
Criminal Appeal of 2005 arising out of SLP(No.1606)of 2004 decided by the supreme Court on Jan 11,2005

[14] Cyber bullying is a negative consequence of online communication between youth. Victims of cyber bullying often experience rumors and lies spread on online social networks. Bullies post inappropriate or uncomfortable pictures of their victims. Another facet of cyber bullying involves using mean text messages as means of harassment both physically and mentally. The National Crime Prevention Council states that cyber bullying is a problem for almost half of American teens where in some extreme cases where teens have taken their own lives as a outcome of cyber bullying.

[15] This is an additional layer of security that requires your user name and the password also a verification code that is sent via SMS to the registered phone number. A hacker may crack the password without the temporary and unique verification code, where one should not be able to access your account. Never share your password to anyone; never send or share any private information like bank account number, ATM pin, password etc over an unencrypted connection including unencrypted mail. Websites that doesn't have the lock icon and https on the address bar of the browser are the unencrypted site. The "s" stands for secure and it indicates that the website is secure; don't sign to any social networking site until and unless one is not old enough; don't forget to update the operating system; firewalls, anti- virus and anti-spyware software should be installed in one's PC and should be regularly updated; visiting to un-trusted website or following a link send by an unknown or by an un-trusted site should be avoided; don't respond to spam; make sure while storing sensitive data in the cloud is encrypted; try to avoid pop-ups as Pop-ups sometimes comes with malicious software as when we accept or follow the pop-ups a download is performed in the background and that downloaded file contains the malware or malicious software and this is called drive-by download. Ignore the pop-ups that offer site survey on ecommerce sites or similar things as they may comprehend the malicious code.

3. Replace the alike character.

While setting the password following things needs to be avoided-

1. Never use a simple password that can easily be decode i.e. password
2. Personal information should never set as a password.
3. Repeating characters should be avoided i.e. aaaacc
4. Using of same password in multiple sites should be avoided. [16]

Cyber Law

Cyber Law took its birth in order to eradicate over the offences committed through the internet or the cyberspace or through the uses of computer resources. Description of the lawful issues that are related to the uses of communication or computer technology can be termed as Cyber Law. Cyber law plays a very imperative role in this new aera of technology. It is important as it is concerned to almost all aspects of activities and transactions that take place either on the internet or other communication devices. Whether we are aware of it or not but each action and reaction in cyberspace has some legal and cyber legal views.[17] Once should have the following knowledge in order to stay aware about the cyber crime:

- One should read the cyber law thoroughly.
- Basic knowledge of Internet and Internet's security.
- Read cyber crime's cases as reading those cases one can be aware from such crimes.
- Trusted application from trusted site can be used for protection of one's sensitive information or data.
- Technology's impact on crime.

The Information Technology Act of India, 2000

According to Wikipedia "The Information Technology Act, 2000 (also known as ITA-2000, or the IT Act) is an act of the Indian Parliament (no 21 of 2000), it was notified on17th October 2000. It is the most important law in India that deals with the digital crimes or cyber crimes and electronic commerce. It is based on the United Nations Model Law on Electronic Commerce 1996 (UNCITRAL Model) recommended by the General Assembly of United Nations by a resolution dated 30 January 1997". Some key points of the Information Technology (IT) Act 2000 are as follows:

- E-mail is now considered as a valid and legal form of communication. Digital signatures are given legal validity within the Act.
- Act has given birth to new business to companies to issue digital certificates by becoming the Certifying Authorities.
- This Act allows the government to issue notices on internet through e-governance.
- The communication between the companies or between the company and the government can be done through internet.
- Addressing the issue of security is the most important feature of this Act. It introduced the construct of digital signatures that verifies the identity of an individual on internet.
- In case of any harm done to the company by criminals the Act provides a remedy in the form of money to the company.[18]
- Whoever intentionally or knowingly destroy, conceal or change any computer's source code that is used for a computer, computer program, and computer system or computer network could be sentenced upto 3 years imprisonment or with a fine of Rs.2 lakhs or with both.[19]
- Hacking with computer system, data alteration etc. Whoever with the purpose or intention to cause any loss, damage or to destroy, delete or to alter any information that resides in a public or any person's computer. Diminish its utility, values or affects it injuriously by any means, commits hacking. Any person who involves in such crimes could be sentenced upto 3 years imprisonment, or with a fine that may extend upto 2 lakhs rupees, or both.[20]
- Sending offensive messages through any communication services- Any information or message sent through any communication services this is offensive or has threatening characters. Any information that is not true or is not valid and is sent with the end goal of annoying, inconvenience, danger, insult, obstruction, injury, criminal intention, enmity, hatred or ill will. Any electronic

[16]Administrative Panel decision of Arbitration &Mediation Centre delivered by panelist W.R Cornish of WIPO on march 11, 2000
[17] State of Punjab vs Gurmit Singh, AIR 1996, SC 1393; The Air Force Bal Bharati, Delhi Cyber Pronographic case (2001)
[18]Peter Stephenson, Investigation computer Related crime. P 85
[19] Section 65 of the IT Act, 2000.
[20] Section 66 of the IT Act, 2000

mail or email sent with the end goal of causing anger, difficulty or mislead or to deceive the address about the origin of the messages. Any individual found to commit such crimeunder this section could be sentenced upto 3years of imprisonment along with a fine.[21]

- Receiving stolen computer's resources or communication devices dishonestly -Receiving or retaining any stolen computer, computer's resources or any communication devices knowingly or having the reason to believe the same. Any person who involves in such crimes could be sentenced either description for a term that may extend upto 3 years of imprisonment or with a fine of rupee 1lakh or both.[22]
- Identify theft -Using of one's digital or electronic signature or one's password or any other unique identification of any person is a crime. Any person who involve in such crimes could be sentenced either with a description for a term which may extend upto 3 years of imprisonment along with a fine that may extend upto rupee 1 lakh.[23]
- Cheating by personation by the use of computer's resources-Whoever tries to cheats someone by personating through any communication devices or computer's resources shall be sentenced either with a description for a term that may extend upto 3 years of imprisonment along with a fine that may extend upto rupee 1 lakh.[24]
- Privacy or violation-Whoever knowingly or with an intention of publishing, transmitting or capturing images of private areas or private parts of any individual without his/her consent, that violets the privacy of the individual shall be shall be sentenced to 3 years of imprisonment or with a fine not exceeding more than 2 lakhs rupees or both.[25]
- Cyber terrorism-[26]Whoever intentionally threatened the integrity, unity, sovereignty or security or strike terror among the people or among any group of people by- Deny to any people to access computer's resources. Attempting to break in or access a computer resource without any authorization or to exceed authorized access. Introducing any computer's contaminant, and through such conducts causes or is probable to cause any death or injury to any individual or damage or any destruction of properties or disrupt or it is known that by such conduct it is probable to cause damage or disruptions of supply or services that are essential to the life of people or unfavourably affect the critical information's infrastructure specified under the section 70 of the IT Act.
- By intention or by knowingly tries to go through or tries to gain access to computer's resources without the authorization or exceeding authorized access, and by such conducts obtains access to the data, information or computer's database which is limited or restricted for certain reason because of the security of the state or foreign relations, or any restricted database, data or any information with the reason to believe that those data or information or the computer's database obtained may use to cause or probably use to cause injury to the interest of the independence and integrity of our country India.[27]Whoever conspires or commits such cyber crime or cyber terrorism shall be sentenced to life time imprisonment.
- Transmitting or publishing obscene materials in electronic form -Whoever transmits or publishing obscene materials in electronic form or whoever publishes or causes to publish any obscene materials in electronics form. Any material that is discourteous or appeal to be lubricious or is likely to be effected it is for instance tends to corrupt any individual who are likely to have regard to all relevant circumstances to read or to see or to hear the matter that contained in it, shall be sentenced on the first criminal with either description for a term that may extend up to five years of imprisonment along with a fine which may extend upto 1 lakh rupee and in the second or subsequent convict it can be sentenced either description for a term that may extend up to ten years along with a fine that may perhaps extend to two lakhs rupees.Prevention is always better than cure. It is always better to take certain protection while operating the net life. Always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs. To prevent cyber stalking avoid disclosing any information pertaining to one self. This is as good as disclosing your identity to strangers in public place. Always keep a watch on the sites that your children are accessing to prevent any kind of harassment or depravation in children. Never send

[21] Section 66A of IT Act, 2000.
[22] Section 66B of IT Act, 2000
[23] Section 66C of IT Act, 2000
[24] Section 66D of IT Act, 2000
[25] Section 66E of IT Act, 2000
[26] Section 66F of IT Act, 2000
[27]Perlord Devlin in Parker knoll vs Knoll International ,1962 RPC 265, UK

your credit card number to any site that is not secured, to guard against frauds. To prevent porn site for children under 18 years. Block pornographic sites on the Internet, which is the primary source of the photos and videos that transmits through Social networking sites.[28]

Conclusion

Recent studies published on the evolution of principal cyber threats in the security concerning scenarios, characterized by the constant growth of cybercrimes activities. Even though the level of awareness of cyber threats has increased and law enforcement acts internationally to combat them. Prohibited profits have reached amazing figures the has impact to society which has become unsustainable. Considering the global economic crisis it is necessary to work together to avoid the costs the global community suffers which we can no longer sustain. The peril of business failure is concrete due to the high cost for enterprises in mitigating counter measures and the damage caused by countless attacks. Nowadays patrons have come to expect that organizations have a presence on the Internet, including a website and e-mail capabilities. Use of the Internet is a risk that most companies have to tackle. If there is no technology hopeful the cybercrimes would not be found anywhere. As it has been discussed in the paper the preventive measures should be undertaken to avert the society as well as the organizations from the cyber crimes instead of avoiding the uses of the technology. It is submitted that since the existence of our society, if it lacks to recognize what cyber bullying is, the suffering of thousands of silent victims will continue without serving its legal measures.

References

1. Details of Treaty No.185 Convention on Cybercrime, Available at http://www.coe. int/ en/ web/conventions/full-list/-/conventions/treaty/185, accessed on 27th August, 2021.
2. J. Clough, A World of Difference, The Budapest Convention on Cybercrime and the Challenges of Harmonisation, Monash, Universal Law Review, 2014
3. S. J. Juneidi, Council of Europe Convention on Cyber Crime.
4. Convention on Cybercrime European Treaty Series No. 185, Council of Europe, XI-2001.
5. Internet Security Threat Report (ISTR), Symantec Corporation World Headquarters 350 Ellis Street Mountain View, CA 94043 United Stated of America, 22nd April, 2017.
6. Carbanak Apt The Great Bank Robbery, Kaspersky, 21st February, 2015.
7. Cybercrime@Coe Update on Council of Europe activities on cybercrime. Jun-2017
8. J. L. 27 M. 2016 at 11:56 tweet_btn(), "Fourth bank hit by SWIFT hackers."
9. The Proofpoint Quarterly Threat Report, Proof point, 2017.
10. 2016-current-state-of-cybercrime. RSA, 2016.
11. S. Morgan, "Hacker pocalypse Cybercrime Report, Cyber Security Ventures, 12th August 2021.
12. Economic Cybercrime, The Next Economic Crime Vector | RSA Conference.

[28] Section 67 of IT Act, 2000