IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cyber Intrusion in India; Challenges and Solutions

Samridhi[1]

Akshara Garg[2]

1 B.Com.LLB 2nd Semester, University Institute Of Legal Studies, Chandigarh
1 B.Com.LLB 2nd Semester, University Institute Of Legal Studies, Chandigarh

Abstract

The Internet is often described as a wonderful tool, an engaging place and a liberating experience but for whom? There is the potential for many of us to become victims to the growing pool of criminals who skilfully navigate the Net. Cyberspace often known as Web is an environment that is intangible and dynamic. This paper argues that Cyber Crime or e – crime presents a new form of business and Hi-tech Criminals. This paper explores an overview of Cyber Crimes, the cyber-crime perpetrators and their motivations also I want to discuss in detail of different cyber crimes, and unique challenges and response issue which may be encountered during the prevention, detection and investigation and also outlined the different section of IT Act 2000 of India also proposed new provision in IT Act 2000. With the rapid development of information technology, people more and more dependent on cyberspace, cyberspace connects billions of users all over the world. It offers great convenience to people; but it also provides a lot of opportunities for criminals to commit crime using the new information tools. Cyberspace has been faced many security challenges like identity tracing, identity theft, cyberspace terrorism and cyberspace warfare. In this paper, we focus on analysis these security challenges, and give some possible solutions offered by law and technology.

Keywords: Cyber Space, Cyber Crime, Hacking, Intellectual Property Rights, [i]Information Technology Act,2000.

1. Introduction

The most important and urgent problems of the technology of today are no longer the satisfactions of the primary needs or of archetypal wishes, but the reparation of the evils and damages by the technology of yesterday." The present situation with regard to cyberspace and the development of the Internet and low-cost wireless communication is similar to Thalidomide; a wonder drug, gone bad. As rightly termed as one of the greatest innovation,

the computer and the internet, are undoubtedly the first amendment brought to life. But this amendment could not control itself within the limits of safe hands, just like an uncontrolled chain reaction, knowing no restriction. The Internet is the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever had.The emergence of the Internet as well as increasing use of information systems have brought about extraordinary changes to human lives. It is transforming many countries‟ growth, dismantling barriers to commerce, and allowing people across the globe to communicate, collaborate and exchange ideas regardless of the traditional barriers of class, geographical location and time. This merger of the internet, information systems and people, now popularly known as the cyberspace has created a global virtual realm for competitive advantage. Worldwide, governments, businesses, organizations, and individuals are increasingly adopting cyberspace technologies for improved productivity and profitability. It is indeed altering socio-economic activities, security postures, and creating opportunities for innovations and prosperity. It has also expanded the means to improve general governance and welfare of the people globally. Indeed, cyberspace has ushered in better options for research, development and innovations, which ultimately is leading to exceptional economic growth and prosperity, as well as enabling informed societies worldwide at an amazing speed (WEF, 2014).

The rising importance of cyberspace to sustain economic growth, delivering of governance to the people, assuring national security and the general prosperity is driving accelerate innovationsto the extent that nowadays virtually every traditional activity has its digital equivalent. We can now trade online, pay bills, play games, carryout banking activities, and communicate back and forth with individuals, businesses and governments. More so, people can be educated online, collaborate and share resources, conduct workshops, seminars, and conferences online, indeed one can control remote sites leveraging online infrastructure.

Life is about a mix of good and evil. So is the Internet. For all the good it does us, cyberspace has its dark sides too. Unlike conventional communities though, there are no policemen patrolling the information superhighway, leaving it open to everything from Trojan horses and viruses to cyber stalking, trademark counterfeiting and cyber terrorism. With the growth of computer technology, the definition of crime is all together changed. A simple click of mouse has given so much power to an anonymous index finger that it can rob millions, crumble a company and even threaten a country's defence. The evolution of technology has impacted the nature of conflict and war. Amongst the recent aspects of involving in conflict is "no contact war" wherein there is no "physical" or "kinetic" action across borders. There is one important nuance in the treatment of cyberspace as a fifth potential theatre of war along with land, sea, air and space. Born out of the merger of two opposite ends of application of human intelligence cyber (the crest of human intelligence) and crime (the trough of human intelligence) cybercrime is giving sleepless nights to the human race.The threats are endless and presently our laws are toothless.

2. Issues that are faced in cyber space

In current scenario cyber crime is increasing very fast as the technology is growing very rapidly. So the cyber crime investigation is becoming a very complicated task to do without a proper framework. There is wide range of different types of cyber crime today.The legal issues that are faced in cyber space can broadly be divided into types are as follows:

Typo squatting :Typosquatting, also known as URL hijacking, is a form of cybersquatting (sitting on sites under someone else's brand or copyright) that targets

Internet users who incorrectly type a website address into their web browser (e.g., "Gooogle.com" instead of "Google.com"). When users make such a typographical error, they may be led to an alternative website owned by a hacker that is usually designed for malicious purposes.This is a practice in cyber space that feeds on the typographic errors of an intending user while searching the domain name of a site. Here a person registers a domain name similar to that of a site with high cyber traffic with minor typo error. These sites are filled with links to paid advertisements that generate revenue for the typosquatter and most of the times, the web surfer tricks or deceive you into believing that you are on the correct site. This diverts traffic away from the intended site and many a times they are routed to a competitor's site or a pornographic site.

Cybersquatting :Cybersquatting is the practice of registering an Internet domain name that is likely to be wanted by another person, business, or organization in the hope that it can be sold to them for a profit. It involves the registration of trademarks and trade names as domain names by third parties, who do not possess rights in such names. Simply put, cybersquatters (or bad faith imitators) register trade-marks, trade names, business names and so on, belonging to third parties with the common motive of trading on the reputation and goodwill of such third parties by either confusing customers or potential customers, and at times, to even sell the domain name to the rightful owner at a profit. This is when someone has registered a domain name, in bad faith, that is violating the rights of the trademark owner. They usually intend to extort payment from the trademark owner, and keeping the names to sell later to the highest bidder.

Pagejacking*:*Pagejacking is a technique used to siphon Internet traffic from intended websites to unintended sites, usually containing pornographic content. Once at the site, surfers might find it difficult to leave, as clicking the "back" button of the browser might only redirect them to new pornographic sites. Pagejacking is unlawful, under the Federal Trade Commission (FTC), falling under the purview of a deceptive practice that interferes with commerce. Pagejacking is when an offender copies parts of an already existing website, and then puts it up on a different website to make it look like the original. Pagejacking is used in phishing schemes.The Uniform Domain Name Dispute Resolution Policy (UDRP) is a cost-effective and faster alternative to a lawsuit, when there is a domain name dispute that needs to be resolved. This was set up by the Internet Corporation for Assigned Names and Numbers (ICANN), the group responsible for domain name registration**.**

3. **Need for cyber law**Jurisdiction is one of the debatable issues in the case of cyber crime due to the very universal nature of the cyber crime. There are various reasons why it is extremely difficult for conventional law to deal with cyberspace.The internet can be seen as a multi jurisdictional because of the ease which a user can access of website anywhere in the world. Millions of websites are being accessed every minute and billions of dollars are electronically transferred around the world by banks every day. A person in India could break into a banks electronic vault hosted on a computer in USA and transfer millions of Rupees to another bank in Switzerland, all within minutes. Steganography has developed a lot in recent years, because digital techniques allow new ways of hiding information's inside other information's, and this can be valuable in a lot of situations. Electronic information has become the main object of cyber crime. It is characterized by extreme mobility, which exceeds by far the mobility of persons, goods or other services.

4. Legal Framework/Statutory Guidelines:

4.1. Protection under Information Technology Act, 2000

The sections of the IT Act, 2000 pertaining to cybercrimes are as follows:

Under the Act, storing or private viewing of obscene material is legal as it does not specifically restrict it. On the other hand, transmitting or publishing the obscene material is illegal. Before 2008, section 67 was the only provision of the Information Technology Act which prohibited the publication of obscene information including child pornography and obscenity. Section 67A of the IT Act, 2000 specifically restricts the publication of sexually explicit or obscene material and section 67B of the Act specifically prohibits child pornography. This section only criminalizes the publication and transmission of sexually explicit or obscene material in an electronic form but viewing, downloading, possession etc. is not an offence as per the provisions of the Act. The main essentials of the section 67 of the IT Act are: (a) transmission of the information in electronic form and (b) that publication appeals to prurient and lascivious interest. This offence is bailable, cognizable and triable by the court of Judicial Magistrate of First Class.

Section 43 – Penalty for damage to a computer, computer system, etc. This section applies if any person, without the permission of the owner or the person in charge of a computer, system, or network –Accesses such computer, network or system.Copies, downloads or extracts any data or information from such computer, network or system (this also includes the information or data stored in a removable storage medium).Also, introduces or causes any computer containment or virus into such computer, network or system.Further, he damages any computer, system or data or any other programs residing in them.Disrupts or causes disruption of any such computer, system or network.Also, denies or causes the denial of access to an authorized person to such computer, system or network.Provides any assistance to anyone to facilitate access to such a computer, system or network contrary to the provisions of the Act and its rules.Also, charges the services availed of by one person to the account of another by tampering with such computer, system or network. The offence is punishable with Compensation, not exceeding one crore rupees to the affected person.

Section 65: This section applies to a person who intentionally conceals, alters or destroys any computer source code used for a computer, program, system or network when the law requires the owner to keep or maintain the source code. It also applies to a person who intentionally causes another person to do the same.Punishable with imprisonment of up to three years or a fine of up to two lakh rupees, also both in some cases.

Section 66: This section applies to a person who commits hacking. Hacking is when the person intentionally or knowingly causes a wrongful loss or damage to the public or another person or destroys or deletes any information residing in a computer resource or diminishes its utility or value or injures it by any means.Punishable with Imprisonment of up to three years or a fine of up to two lakh rupees, also both in some cases.

Section 67: This section applies to a person who publishes or transmits any obscene material – material which is lascivious or appeals to the prurient interests or tends to deprave or corrupt persons who are likely to read, see or hear the matter embodied in it. It also applies to a person who causes the publishing or transmission of such material.The offence is punishable in case of the first conviction, imprisonment of up to five years and a fine of up to one lakh rupees. For subsequent convictions, imprisonment of up to 10 years and a fine of up to two lakh rupees.

Section 74: This section applies to a person who knowingly creates, publishes or makes available a digital certificate with the intention of fraud.The offence is punishable with Imprisonment of up to two years or a fine of up to one lakh rupees, also both in some cases.

Section 44 : This section applies to a person who Fails to furnish any document, return or report to the Controller or the Certifying Authority Fails to file returns or furnish any information as per the regulations or fails to furnish them in time Does not maintain the books of account or records. The offence is punishable with a fine of up to five thousand rupees for every day if the failure continues. A fine of up to ten thousand rupees for every day if the failure continues.

Section 45 : This section applies to a person who contravenes any rules under the IT Act, 2000, especially those for which there are no special provisions. The offence is punishable with a compensation of up to twenty-five thousand rupees to the affected person.

Section 71: This section applies to a person who makes any misrepresentation to or even suppresses any material fact from the Controller or Certifying Authority to obtain the license or a digital signature certificate. The offence is punishable with Imprisonment of up to two years or a fine of up to one lakh rupees, also both in some cases.

Section 72 : This section applies to a person with secured access to any electronic record, information, or any other material, discloses it to another person without consent. The offence is punishable with imprisonment of up to two years or a fine of up to one lakh rupees, also both in some cases.

Section73:Publishing a Digital Certificate with incorrect details. This section applies to a person who publishes a digital certificate with the knowledge that – The Certifying Authority listed in the certificate has not issued it.The subscriber listed in the certificate has not accepted it .It is a revoked or suspended certificate. The offence is punishable with imprisonment of up to two years or a fine of up to one lakh rupees, also both in some cases.

Section 74: This section applies to a person who knowingly creates, publishes or makes available a digital signature for fraudulent purposes. The offence is punishable with imprisonment of up to two years or a fine of up to one lakh rupees, also both in some cases.

Section 85:This section applies to a company who commits a contravention to the provisions of the Act. In such cases, all the people who were in charge and responsible for the company's conduct of business as well as the company are guilty of the contravention. Further, those responsible are liable for punishment.

However, if a person is not aware of any such contravention, then he is not liable, if it is proved that the contravention was with the consent of, or due to the negligence of any director, manager or any other officer, then such people are also held liable.For the purposes of this section, "company" means any body corporate and also includes a firm or other association of individuals.

4.2. **CERT-In:**Under Section 70B of the IT (Amendment) Act 2008, the government constituted CERT-In, which the website of the Ministry of Electronics and Information Technology refers to as the 'Indian Computer Emergency Response Team'. CERT-In is a national nodal agency responding to computer security incidents as and when they occur. The Ministry of Electronics and Information Technology specifies the functions of the agency as follows:(a)collection, analysis and dissemination of information on cybersecurity incidents.(b)forecast and alerts of cybersecurity incidents.(c)emergency measures for handling cybersecurity incidents.(d)coordination of cybersecurity incident response activities; and issuance of guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response to and reporting of cybersecurity incidents.

4.3. **Cyber Regulations Appellate Tribunal (CRAT)**Under Section 48(1) of the IT Act 2000, the Ministry of Electronics and Information Technology established CRAT in October 2006. The IT (Amendment) Act 2008 renamed the tribunal Cyber Appellate Tribunal (CAT). Pursuant to the IT Act, any person aggrieved by an order made by the Controller of Certifying Authorities, or by an adjudicating officer under this Act, may prefer an appeal before the CAT. The CAT is headed by a chairperson who is appointed by the central government by notification, as provided under Section 49 of the IT Act 2000.Before the IT (Amendment) Act 2008, the chairperson was known as the presiding officer. Provisions have been made in the amended Act for CAT to comprise of a chairperson and such a number of other members as the central government may notify or appoint.

4.4. **Parliamentary Report on Cyber Security & Right to Privacy:** The Parliamentary Standing Committee on Information Technology in its 52nd Report on Cyber Security and Right to Privacy said that a significant increase in cyberspace activities and access to internet use in India coupled with lack of user end discipline, inadequate protection of computer systems, and the possibility of anonymous use of ICT allowing users to impersonate and cover their trends of crime has emboldened more number of users experimenting with ICT abuse for criminal activities. The Committee is of the opinion that this aspect has a significant impact in blunting the deterrence effect created by the legal framework in the form of the Information Technology Act, 2000, and allied laws.

The Committee has listed several offenses which fall under the purview of cyber-crimes and the remedies available within the existing legal framework. Cyberstalking or stealthily following a person and tracking his internet chats is punishable under Sec 43 and 66 of the IT Act, 2000 while video voyeurism and violation of privacy is a crime under Section 66E of the IT Act with a punishment of three years with fine. The Department of Electronics and Information Technology (DeiTY) during the course of evidence submitted to the Committee

that with regard to the data pertaining to privacy related cases booked under Sec 72(A) of the IT Act.

The Committee members were of the opinion that considering the nature of cyberspace which is borderless, balancing cybersecurity, cyber-crime and the right to privacy is an extremely complex task. The members were also unhappy of the fact the government is yet to institute a legal framework on privacy. It urged upon the Department of Electronics and Information Technology (DeiTY) in coordination with the Department of Personnel and Training and multi-disciplinary professionals/experts to come out with a comprehensive and people-friendly policy for the protection of the privacy of its citizens.

5. **Indian Penal Code:**Section 378 of the IPC relating to "theft" of movable property will apply to the theft of any data, online or otherwise, since section 22 of the IPC states that the words "movable property" are intended to include corporeal property of every description, except land and things attached to the earth or permanently fastened to anything which is attached to the earth. The maximum punishment for theft under section 378 of the IPC is imprisonment of up to 3 (three) years or a fine or both.It may be argued that the word "corporeal" which means 'physical' or 'material' would exclude digital properties from the ambit of the aforesaid section 378 of the IPC. The counter argument would be that the drafters intended to cover properties of every description, except land and things attached to the earth or permanently fastened to anything which is attached to the earth.

Section 424 of the IPC states that "whoever dishonestly or fraudulently conceals or removes any property of himself or any other person, or dishonestly or fraudulently assists in the concealment or removal thereof, or dishonestly releases any demand or claim to which he is entitled, shall be punished with imprisonment of either description[1] for a term which may extend to 2 (two) years, or with fine, or with both." This aforementioned section will also apply to data theft. The maximum punishment under section 424 is imprisonment of up to 2 (two) years or a fine or both.

Section 425 of the IPC deals with mischief and states that "whoever with intent to cause, or knowing that he is likely to cause, wrongful loss or damage to the public or to any person, causes the destruction of any property, or any such change in any property or in the situation thereof as destroys or diminishes its value or utility, or affects it injuriously, commits mischief". Needless to say, damaging computer systems and even denying access to a computer system will fall within the aforesaid section 425 of the IPC. The maximum punishment for mischief as per section 426 of the IPC is imprisonment of up to 3 (three) months or a fine or both.

5.1. **Data Protection Bill 2019**

The Personal Data protection Bill 2019 (PDP) is India's first law on the protection of data and it will repeal section-43A of the IT Act. The PDP Bill, proposes a broader reach. It will not only apply to persons in India but also to persons outside India in relation to business carried out in India. The PDP Bill, proposes to apply both on manual and electronic records. The PDP bill proposes creating a data protection authority in India. The authority will be responsible for protecting the interest of data principals, preventing misuse of personal data and ensuring compliance within the new law. The PDP Bill proposes to protect personal data relating to the identity, characteristics trait, attribute of a natural person and Sensitive Personal Data such as financial data, health data, official identifier, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex

status, caste or tribe, religious or political beliefs. Pursuant to the PDPB being enacted into an Act, there are several compliances to be followed by organizations processing personal data in order to ensure the protection of privacy of individuals relating to their Personal Data. Consent of the individual would be required for the processing of personal data.

Based on the type of personal data being processed, organizations will have to review and update data protection policies, codes to ensure these are consistent with the revised principles such as update their internal breach notification procedures, implement appropriate technical and organizational measures to prevent misuse of data, Data Protection Officer to be appointed by the Significant Data Fiduciary, and instituting grievance redressal mechanisms to address complaints by individuals.In a Landmark Judgement delivered on August 23rd 2017, **Justice K.S Puttaswamy (Retd.) Versus Union of India** (Case NO- WP (C) 494/2012), the Hon'ble Supreme Court through its 9 Judge Bench held that the fundamental right to privacy is guaranteed under the Constitution of India.The Court stated that every person should have the right to control the commercial use of his or her identity and that the right of an individual to exclusively use and commercially exploit their identity and personal information, to control the information that is available about them on the internet and to disseminate certain personal information for limited purposes only which emanate from this right. This is for the first time Supreme Court has expressly recognized the right of an individual over his personal data.

5.2. Preventive approach of cyber crime

India should consider organised crime strategies to include cyber offences committed by means of computer system. The action plan should include activities for the authorities responsible with prevention and fighting against cybercrime including cybersecurity in order to implement the main concepts from the cybersecurity strategy (define critical infrastructure, create the early warning system, coordination body/entity for cyber incident/attacks, response procedures). Without detailed action plans listing the necessary responsible actors and resources for implementation, the cybercrime or cybersecurity strategies remain the statements of intent. Due to the cross border characteristics of cybercrime, the solution of cyber crime cases requires the support of other states. But, international cooperation can be structured on different levels: the cybersecurity strategy should specify the competence of particular authorities in the domains of NIS, cybercrime or cyber defence. A multi-stakeholder approach is an essential element of cybersecurity strategies. For the implementation of this approach, all national stakeholders from the public and private sector should be involved in the development, implementation and enforcement of a cybersecurity strategy. Different strategies for cybercrime and cybersecurity could be an option but a mechanism for coordination and cooperation between different authorities should be implemented.Therefore, increased collaboration between government entities at national and international level is absolutely vital for the success of a holistic ‘cyber’ approach in executing a cyber strategy.

5.3. Conclusion

Due to diversified nature it is difficult to identify the cyber security problems which leads to unawareness on security issues. The proliferation in registering the cybercrimes under various sections of IT act and IPC shows the severity of such

cyber threats however most of the cases were still unreported because of various reasons. Policies or strategies should be based on knowledge of cyber threats, problems and challenges, as well as informed decision understanding the actual threats and challenges of cyberspace.

REFERENCES

1. Cyber Space Jurisdiction: Issues and Challenges.Avialable athttps://www.legalbites.in/cyber-space-jurisdiction-issues-challenges/ Last assessed on 30 March, 2021.
2. Cybercrime and cybersecurity strategies in the Eastern Partnership region. Avialable at https://rm.coe.int/eap-cybercrime-and-cybersecurity-strategies/168093b89c. Last assessed on 30 March, 2021.
3. New Generation of angry & Youthful hackers join the hacktivism wave,adding to cyber-security woes.Available at https://economictimes.indiatimes.com/magazines/panache/new-generation-of-angry-youthful-hackers-join-the-hacktivism-wave-adding-to-cyber-security-woes/articleshow/81707844.cms. Last assessed on 30 March, 2021.
4. Justice K.S.Puttaswamy(Retd) vs Union Of India And Ors. on 24 August, 2017.Available at https://indiankanoon.org/doc/91938676/. Last assessed on 30 March, 2021
5. Report on Cyber Security & Right to Privacy submitted by the Parliamentary Standing Committee on Information Technology Act presented on Feb 12th 2014, under the chairmanship of Rao Inderjit Singh to the fifteenth of the Lok Sabha.
6. The categories of the crimes have been adapted from the article found in https://www.lawctopus.com/academike/cyber-crimes-other-liabilities/ Last assessed on 30 March, 2021
7. Cyber space available at: https://www.britannica.com/topic/cyberspace. Last assessed on 28 March, 2021
8. Barkha, Rama Mohan, U. (2011) Cyber Law and Crimes, IT Act 2000 & Computer Crime analysis. (3rd ed.), ISBN: 978-93-81113-23-3.
9. India: Key Features Of The Personal Data Protection Bill, 2019 available at https://www.mondaq.com/india/data-protection/904330/key-features-of-the-personal-data-protection-bill-2019. Last assessed on 28 March, 2021
10. Examining the importance of Stenography information technology essay. Available at https://www.ukessays.com/essays/information-technology/examining-the-importance-of-steganography-information-technology-essay.php. Last assessed on 28 March, 2021
11. Introduction to Cyber Crime, Available at: http://cybercrime.planetindia.net/cybercrime_cell.htm. Last assessed on 28 March, 2021.
12. Legal Service India < http://legalservicesindia.com/article/article/offences-&-penalties-under-the-it-act-2000-439-1.html> last assessed on 2 Octobe, 2012.
13. Cyber Space Jurisprudence, Available at https://www.coursehero.com/file/p6qh84m/2-Cyberspace-has-complete-disrespect-for-jurisdictional-boundaries-A-person-in/ last assessed on 31 March, 2021.