Journal Global Values, Vol. XV, No. 2 2024, ISSN: (P) 0976-9447, (e) 2454-8391, Impact Factor 8.888*(SJIF)*
https://doi.org/10.31995/jgv.2024.v15i02.023

Cybercrime, Cyberspace and Cyber Security

Lakhendra Kumar Chhokar
Research Scholar
School of Legal Studies,
Jigyasa University, Dehradun
(Formerly Himgiri Zee University)
Email:adlakhindra@gmail.com

Dr. Shalini Bahuguna Bachheti
Dean
School of Legal Studies
Jigyasa University, Dehradun
(Formerly Himgiri Zee University)

Abstract

The staggering use of information technology in the general public and dependency on web usage in all around the world is at the edge. Cybercriminals are not constrained by boundaries as the internet is borderless and free streaming at globally. Cybercrime includes to all criminal events occurring through the internet and computer. Growth in technology has changed the overall economy, market and related people's habits. With the data progression, countries across the world are examining different courses as to creative considerations and extensive improvement. The web can be depicted as a confusing climate that integrates relationships between individuals, programming additionally and associations. Cybersecurity means to provide protection from computerized assaults to the computer programs, software, cyber networks and data which is stored in the server as well as computers.

Keywords

Cybercrime, Cyberspace, Cyber Security, Data protection.

Reference to this paper should be made as follows:
Received: 11.09.2024
Approved: 20.12.2024

Lakhendra Kumar Chhokar
Dr. Shalini Bahuguna Bachheti

Cybercrime, Cyberspace and Cyber Security

Vol. XV, No.2
Article No.23,
pp. 211-217

Similarity Check: 09%

Online available at
https://anubooks.com/journal/journal-global-values

DOI: https://doi.org/10.31995/jgv.2024.v15i01.023

1. Introduction

In this technical era technology is expanding beyond the assumption of human beings worldwide. The unbelievable development of information society and its reliance on web utilization in all over the world is along the side joined by the weakness of social orders to cybercrime. Information technology gives an open door to the wrongdoer to carry out conventional violations like cheating, misrepresentation, misappropriation of bank deposits, MasterCard, credit card fraud, modern and political surveillance and so on. Simultaneously, it additionally helps in executing forward-thinking data innovation explicit assaults, against the security of basic frameworks like telecom, banking or crisis administrations, national security etc. Such wrongdoings might be carried out through computer networks across the public lines, influencing not mere people, they may rather bring about compromising the security and economy of the country. The Cyber security dangers exude from a wide assortment of sources and manifest themselves in troublesome exercises that target people, organizations, public frameworks and State-run administrations the same.

2. Objective of The Study

The main objective of this research study is to know the nature and scope of Cybercrime, Cyberspace and Cyber Security.

3. Nature of Cyber Crime

Bad behavior is a socially related understanding. Regardless of what the total we attempt, in the present technical age we can't encounter a general populace without cybercrime. In a genuine sense, when we are not yet ready to control the bad behavior rate to the positive least really, how would it be a good idea for it is within the realm of possibilities to really look at a relative in the virtual world, as the indistinguishable is truly stunning, constant and honestly less controllable. In any case with the time, nature and degree and importance of bad behavior changes in a given society. Crime-free society is a myth and bad behaviour can't be disengaged from an overall population. In this manner the possibility of the bad behavior depends on the possibility of an overall population. The unpredictability of the overall population concludes the multifaceted design of the bad behavior that is created around it. To fathom the bad behavior in an overall population, it is key and dire to affirm all of the factors that affect and add to the bad behavior.

The progress of the advancement has conveyed new monetary and policy-driven issues in the overall population and well actually of supporting the state in controlling the issue it has caused a new complex situation, which is difficult to appreciate and, shockingly, more testing to apply flow guideline to defy what is

happening. The state hardware isn't furnished with an adequate number of sources and information to deal with the cutting-edge cybercrime.[1]

Computers have changed the advanced society beyond assumptions in the last three to four decades. It has made life advantageous as well as colossally helped various areas of the world draw nearer socially, monetarily and culturally. The PC innovation has made it conceivable to approach all edges of the world while sitting in a room. Present-day innovation has stopped the obstructions of reality. Nonetheless, improbable with the striking benefits of having PCs today, because of this the jurisdictional issue has been made in the general set of laws.

Jurisdiction is one viewpoint that is truly challenging to decide in transnational exchange over the web. There was unmanageable vagueness when courts were exposed to questions relating to locale regulation and couldn't choose the appropriate gathering to engage cases including digital wrongdoing as the internet or virtual world is borderless assuming we contrast it and the actual world and for that reason controlling cybercrime is extremely challenging.

In this manner, the worldwide component of digital wrongdoing has made it challenging to deal with and manage. The advancement of web innovation has given us such countless benefits to manage future issues and develop at a fast rate yet additionally it has given the degree to crooks to carry out their wrongdoing with the least possibility of identification. The internet has demonstrated a shelter to the degenerate conduct of the general public.

4. Types of Cybercrime

The United States of America is the birthplace of the Internet and experienced the first computer-facilitated crime in the year 1969.[2] In the United Kingdom, the Computer Misuse Act, of 1990[3] Has categorized cybercrimes into three categories:

- Offenses against the confidentiality, integrity and availability of computer data and systems
- Computer Related Offences
- Content Related Offences

In India the digital violations are given under chapter XI of the Information Technology Act, 2000[4] Under the heading of 'Offenses' which manages the different kinds of offenses that are finished in the electronic structure or worried with PCs, Computer frameworks, and computer networks. Hereunder are referenced those digital violations that are punishable under the Information Technology Act, 2000 under independent sections.

These are as follows:

- Tampering with computer source documents
- Computer related offences
- Sending offensive messages through communication service
- Dishonestly receiving stolen computer resources or communication device
- Identity Theft
- Cheating by personation by using computer resource
- Violation of privacy
- Cyber terrorism
- Publishing of information, which is obscene in electronic form
- Publishing or Transmitting of Obscene Material in Electronic form
- Hacking
- Cyberstalking
- Cyber defamation

Besides above mention crimes there are other cybercrimes that are the result of the advanced technology which is increasing day by day and the use of this technology by human beings to furnish their work in various fields with speed and accuracy. In mean meantime it provides new criminal opportunities to wrongdoers to cybercrime. These are the following:-

- Forgery
- Computer Vandalism
- Virus
- Fraud by computer Manipulation
- Web defacement and denial of Service Attacks-
- Liability of ISP's (Internet Service provider)
- Tools for Cyber attackers

Digital aggressors utilize various weaknesses in the internet to commit these demonstrations. They exploit the shortcomings in programming and equipment plans using malware. Such as, Bluetooth hijacking, Boot net, Browser hijacking, E-mail address harvesting, e-mail-related crime, Keyboard logging etc.

5. Concept of Cyberspace

A science fiction writer, William Gibson is known to have used the word 'Cyber' in his Novel Neuromancer 1984[5], but he had actually invented it years ago in a short story, which appeared in the Omni magazine. Cyber, as a prefix, first

appeared in the word cybernetics in 1948, which was coined by Norbert Weiner in his book of the same name Weiner derived it from the Greek word for steersmen and the idea of control is central to it. The meaning of cyber has evolved over the past decade. Its original sense in Neuromancer was of electronic space, as perceived by what we now know as visual reality. "Cyberspace" was originally used for electronic space. The brain and senses were directly linked with the world of computers and communications and so could experience it as an actual landscape. Later on it was used for intangible electronic domain. Now it is being used, as a loose synonym for electronic cyberspace, therefore, it is a place where two people meet, not physically but virtually and communicate with each other electronically. Organizations and individuals have sued each other in long-drawn court, battles over the rights to control this overwhelming space.

Crimes have been perpetrated right from the ancient days. History tells us about various laws and codes that were framed by different rulers and the way punishments were awarded to the offenders. Some of the investigations have been righteous while others have been inhuman and cruel. Before the advent of computer crimes, the law enforcement agencies were bound by some ground rules. There were established procedures for the investigation and prosecution of all types of crimes. In the case of traditional crimes, large number of physical evidence is generally available at the scene of crime. Collection of such physical evidence material needed a lot of common sense and a little technical knowledge. Forensic assistance could also be provided easily since the laboratory examination procedures are fully established. The crime scene is also confined to a relatively smaller place.

Whether it is a local area network (LAN), a wide area network (WAN) or the World Wide Web (www) they are fertile grounds for the mushrooming of criminal deeds that would pose a serious threat to public welfare, morality and the justice delivery system of the country. Nations at war would increasingly depend on crippling the enemy through sabotage of the information system[6]. Various surveys indicate that the attacks on the computer systems are going to increase manifold through telecommunication networks, theft of telecommunication services and the use of computers to commit crimes of data manipulation.

The Indian Cyberspace

The National Informatics Centre (NIC) was set up as early as 1975 with the goal of providing Information Technology solutions to the government[7].

6. Cyber Security

The cyber security perils emanate from a wide combination of various sources. Which targets individuals, associations, public establishments and Councils

and also causes problems to their assets. The beginning of an impedance emerges from the character of the blameworthy party yet inspiration for it will showing can occur from in a general sense any place. These convey dangerous basic bets to destroy public prosperity, the security of the nation and the strength of the universally associated economy in general.

Cyber Security is "the security of information and its communicating channels as applied to computing devices such as computers and smartphones, as well as computer networks such as private and public networks, including the Internet as a whole."[8]

The field covers every one of the cycles and components by which personal computer-based gear, data and administrations are shielded from accidental or unapproved access, change or annihilation. Personal computer security too incorporates security from spontaneous occasions and cataclysmic events.

Cyber security is a mind-boggling issue that cuts across numerous spaces and calls for multi-layered, diverse drives and reactions. It has demonstrated a test for states from one side of the planet to the other. The errand is made troublesome by the undeveloped and diffuse nature of the dangers and the powerlessness to approach a satisfactory reaction without a trace of unmistakable culprits. The velocity in the improvement of data innovation and the general simplicity with which applications can be popularized has seen the utilization of the internet grow emphatically in its short presence.

7. Conclusion

The tremendous advancement of web users in the world, particularly India is along the side joined by a huge flood in cybercrime and has made India vulnerable to such. Cybercrimes are of a worldwide nature and crooks are not bound to a particular geological region. The internet is a free streaming, borderless and not safeguarded by neighborhood offenders. Various issues associated with human beings and the Organizations become apparent, when most of the activities are carried out on the web. In such a case more criminal activities related to the web also will be increased. A couple of central moral issues related to the usage of Information Technology include individual security, data access information and perilous exercises Online. Computerized bad behavior is a kind of offense that deals with the cyber world and integrates personal computer security, information security, and flexible security too. The rising number of infringements in the field of Information communication technology brings an enormous risks for all the users. So the use of the internet must be limited to the requirement.

References

1. Severino, J. M., & Ray, O. (2009). The end of ODA: death and rebirth of a global public policy. *Available at SSRN 1392460*
2. Talat Fatima, Cyber Crimes, 2011, Pg. **454**
3. Button, M., Shepherd, D., Blackburn, D., Sugiura, L., Kapend, R., & Wang, V. (2022). Assessing the seriousness of cybercrime: The case of computer misuse crime in the United Kingdom and the victims' perspective. *Criminology & Criminal Justice,*17488958221128128.
4. Udapudi, S. V., & Ghosh, B. (2012). The Information Technology Act of India: A Critique. *ZENITH International Journal of Business Economics & Management Research, 2*(5), Pg. **182-194.**
5. Wall, D. S. (2012). The devil drives a Lada: The social construction of hackers as cyber criminals. *Constructing Crime: Discourse and Cultural Representations of Crime and 'Deviance'*, Pg. **4-18.**
6. Adams, J. (2001).*The next world war: Computers are the weapons and the front line is everywhere*. Simon and Schuster.
7. Verma, N., & Kumaran, G. M. M. (2021). Digital Transformation in Government—A Case Study of India. In *Citizen Empowerment through Digital Transformation in Government* Pg. **1-22**. Chapman and Hall/CRC.
8. Hossain, M. M., Fotouhi, M., & Hasan, R. (2015, June). Towards an analysis of security issues, challenges, and open problems in the Internet of Things. In *2015 ie World Congress on Services* Pg. **21-28**. IEEE.