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

CYBERCRIME IN CYBERSPACE AND CONCERN RAISED BY HUMAN RIGHTS: AN OVERVIEW

SWATI YADAV[1] **DR. BRIJESH KUMAR**[2]

RESEARCH SCHOLAR **PRINCIPAL (Retd.)**

CMP DEGREE COLLEGE,

UNIVERSITY OF ALLAHABAD,

PRAYAGRAJ, INDIA.

ABSTRACT

While providing us with many opportunities, the development of digital technology has also created a number of issues, such as cybercrime. Because there is a genuine risk of information breaches, this has raised alarm among the general public. The growth of cybersecurity is a result of this. The study tries to demonstrate the importance of accurately defining the term "cybersecurity." Furthermore, it explains the value of cybersecurity and why it is essential in the current digital environment. The study focuses on various cybersecurity regulations and how they influence human rights, as well as how people respond to having these laws imposed upon them.

Keywords: *Cybersecurity, Vigilance, NIPS, Human Rights, Cybercrime, Electronic monitoring.*

INTRODUCTION

The security and stability of cyberspace, including the Internet, are frequently the pillars on which conversations about cybersecurity, Internet governance, and Internet freedom rest, from the first computer worm that surfaced in the late 1980s to the most recent Sony Pictures Entertainment attack in 2014. Cybercrime, spam, identity theft, data breaches, computer viruses, and denial-of-service assaults are just a few examples of potential threats. Attackers can include business entities, national governments, petty criminals, hackers, activists, and others. Online risks to our human rights are just as real as those to our security, with tens of thousands of identified infections and over 370 million people falling victim to cybercrimes yearly.

According to the Internet Society (ISOC), "cybersecurity" has been called “a term that is horrifyingly vague and can refer to an almost unlimited range of diverse security issues, technological difficulties, and "solutions" ranging from the technological to the legislative.” While terms like “cybersecurity” may make for catchy headlines, a standard grasp of what it means is necessary for serious debates on security and the Internet.

Information security, cybersecurity, cyberwarfare, cyber surveillance, and many more terms have not been standardized by a legally binding international organization or alliance. It follows that different parties use these terms in diverse contexts, which facilitates policy discussions and makes it easier for some governments to violate fundamental rights under the guise of a serious "cybersecurity" danger. A project to gather cybersecurity-related terms in the Global Cyber Definitions Database was funded in 2014 by the Swiss government. Understanding the fundamentals of cybersecurity depends on the following words: "cyberspace, "internet, and information security." Critical infrastructure, cybercrime, cyberwarfare, cyberspace, and hacktivism are all examples of cybersecurity. (Carolina Rossini and Natalie Green, 2015)

REVIEW OF LITERATURE

Brenner (2004) explained the first technique for figuring out criteria for rating online criminal activity. She suggests a straightforward taxonomy of damages consisting of three primary forms, namely individual, systemic, and global, even though she accepts that it is very difficult to establish criteria and levels for cybercrime because of the "fear or anxiety," size, and evidence concerns.

Using a Bayesian generalized linear model, a public information database of security breaches is used by **Edwards *et al. (2016*)** to discover trends in data breaches. They come to the conclusion that, although the volume and number of data incidents have stayed the same in recent years, threat actors are nonetheless affected by them as they get more adept at making money off of the sale of personal data and as the volume of electronic financial transactions rises.

According to **Dr.Yusuf Perwej *et al*. (2021)** , network and application software, security software, and software for personal and professional devices should be updated regularly. A simulation-based training scenario is presented in which student trainees practice their response in a virtual environment with the goal of preparing them for actual attacks. To simulate the symptoms and effects of a DDoS attack, a simulator, and hacking tools are used.

Nguyen *et al.* (2017) provided an intriguing strategy based on the “top-down” paradigm discussed in the criminology area. The authors made an effort to elicit “premiums” that certain users could be prepared to pay in order to safeguard their assets from cyber incidents. Our current understanding of cybersecurity mainly relies on information from news reports and business threat reports. Nevertheless, this information only provides us with a partial and distorted picture of the activities surrounding cyber dangers since it is usually politicized and influenced by the needs of powerful customers and the interests of knowledgeable suppliers.

OBJECTIVES OF THE STUDY

- To know cybercrime and its challenges.
- To make individuals vigilant and aware of surroundings.
- To create concerns raised by human rights.

CONCERNS ABOUT CYBERSECURITY RAISED BY HUMAN RIGHTS

Despite the fact that a number of national and international laws attempt to include human rights concerns when developing cyber security standards, civil society activists and others have realized the danger that comprehensive and extensively used cyber security laws and principles pose to human rights.

The International Covenant on Civil and Political Rights (ICCPR) and the Universal Declaration of Human Rights (UDHR) provide a variety of rights, including freedom of expression, freedom of speech, the right to privacy, freedom of thought, and freedom of association. The UN Special Rapporteur on Freedom of Opinion and Expression, as well as rapporteurs on freedom of expression from Europe, Latin America, and Africa, jointly

declared in 2011 that "freedom of expression applies to the Internet" in response to the growth of the Internet as a new medium for the expression of fundamental human rights.

The UDHR and ICCPR human rights declarations are now applicable to the Internet after the UN Human Rights Council reiterated in July 2012 that “the same rights that people have offline must also be protected online."

Many nations have adopted cyber security laws and policies that may negatively impact online speech and freedom of expression, either directly impinging upon those rights or chilling people's desire to exercise those rights. The Anti-Cyber Crime Law in Saudi Arabia, with its ambiguous reference to the "protection of public interest, morals, and common values," has been used to censor online speech and imprison bloggers and others for expressing opposing views, making fun of public figures, or supporting organizations in an effort to suppress internet speech and freedom of expression by parties other than the ruling government.

NIPS (NETWORK INTRUSION PROTECTION SYSTEM)

The phrase serves as a catch-all for a collection of hardware and software technologies that guard computer networks against unauthorized access and destructive behavior.

Network Intrusion Detection System (NIDS)

A network intrusion detection system (NIDS), an intrusion prevention system (IPS), or a hybrid system like an intrusion prevention and detection system (IPDS) can all be used to detect intrusions.

Note that an IPS can actively halt an attack by following established rules, such as changing firewall settings, blocking specific Internet protocol (IP) addresses, or completely dropping certain packets, but a NIDS can simply detect intrusions.

CYBERCRIME

In essence, there are three categories of crime in this world: cybercrime, digital crime, and computer crime. "Digital crime" is the broadest definition of crime, which includes all criminal action using digital tools or targets. Any criminal activity that targets, employs, or includes computers incidentally is referred to as computer crime. Cybercrime is a phrase used to describe offenses done online, particularly in network environments. Data tampering, credit card fraud, spoofing, denial-of-service assaults, online pornography, net extortion, and data mining are examples of cybercrime types. Examples of various forms of cybercrime include software piracy, salami attacks, support for terrorism, cryptography, and Nigerian fraud (419).

The term "hacking" describes unlawful access to a computer system without the user's permission (sometimes referred to as "cyber trespass" or "intrusions"). Yet, it also replaces the victim's wrongful loss or harm and deletes or edits any data that has been saved in a computer resource. can include harm, gains, data destruction, manipulating debit or credit accounts or restrictions, and mischief. Hacking is punishable under Section 66 of the Information Technology Act.

One might ask: Where does cybercrime occur? is the Digital Information Highway (DIH). What is "the digital information highway," then? Anywhere that digital stamping, such as telephony/mobile, the internet, email, social networking, internet banking, or online shopping/reserving, takes place is DIH. Cards for credit, cash, virtual (e-wallets), CC TV, Telecom Networks: Land Line, Cellular, and Satellite Phones, and so forth.

Evidence

As deleted data is exceedingly difficult to recover, networks maintain very accurate records of transactions, and computers keep very meticulous records of what transpired in crime and technology's unrestricted information flow, global, immediate, anonymous, hard to track, and virtual presence.

INVESTIGATION OF CYBERCRIME: CHALLENGES

The two main dangers of web services are identity theft and rumor spreading. It results in traditional crimes, impersonation, defamation, instigation, financial fraud, and more.

What methods do hackers use to exploit social networking sites?

It is important to highlight that web services offer a huge opportunity to obtain digital evidence. Internet and mobile usage privacy, tools, and services used in crime are kept on servers outside of India. A federal crime's nature, victim, perpetrator, enabler, and beneficiary in diverse places, tracking criminals using forensics and technological monitoring, Less prepared are banks, police, and the judiciary, which have difficulties with the case presentation. The utilization of mobile data, IMEI digits, cell ID data, ICR, and an IPDR-NATed IPv4 structure utilizing voice matching intercepted and natural sample matching are the steps taken.

ELECTRONIC MONITORING

Electronic surveillance involves keeping an eye on digital stamps. Electronic monitoring has become a crucial instrument as the usage of digital methods of communication and commerce has increased. Mobile, email, ATM/internet banking/credit cards, train/airline booking, money transfer, amateur images, and videos are all examples of digital stamping. Electronic forensics digital forensics Mobile forensics stores data such as cell phone logs, address books, planners, messengers, cameras, GPS devices, and web clients. Website for third-party and email forensics.

CONCLUSION

Even though India has many laws to prevent cybercrime, they all seem to be ineffective. Hackers always develop new methods to circumvent cybersecurity and steal crucial data. Government policy should be written so as not to violate fundamental human rights. An analysis of legal and ethical positions and practices must be done in conjunction with issues relating to surveillance, communications monitoring, privacy, consent, and technology. Only then would there be an opportunity to protect fundamental human rights and enhance accountability in today's highly developed technological world. Several institutions must now take steps to stop this contagious kind of cybercrime. Being vigilant means keeping an eye on your surroundings. Establishing routines and habits that promote ongoing watchfulness and allow you to assess how you are doing in terms of secure behavior is the key to keeping vigilant in your daily affairs. SOPs.Until and unless an individual is vigilant, which is why we should keep watch: for self-worth, prudence, and security.

Threat

Why? because of avarice, a sadistic mindset, or unlawful money-making. how to hypnotize someone to cheat in any way or gain unauthorized access (all sorts of identity theft). Where there is mischief, disruption, harm to reputation or character, harm to competitors in the field, earning money.

What dangers are there?

Hypnotism: how to hypnotize someone to cheat in any way or gain unauthorized access (all sorts of identity theft). Tappebazi: The Real World Self/ family/ property-Home and Office Security-House Breaking/ Snatching/ Looting/ Dacoit/ Extortion/ Kidnapping/ VehicTheft/etc. Document cheating or impersonation, Internal security is incredibly well organized and impotent, which is a problem for the security forces. Unauthorized access in the digital world Phishing, vishing, and pharming are all ways of committing crimes via obtaining valid information and credentials. Theft of identity.

REFERENCES

- Brenner SW. Cybercrime metrics: old wine, new bottles? Va. JL & Tech, 9:13–13, 2004.
- CAROLINA ROSSINI AND NATALIE GREEN, PUBLIC KNOWLEDGE.
- Dr.Arwind Chaturvedi,SP Vigilance,Cyber Security Workshop,IMS,University of Lucknow.
- Dr.Yusuf Perwej, Syed Qamar Abbas, Jai Pratap Dixit, Dr. Nikhat Akhtar, Anurag Kumar Jaiswal. A Systematic Literature Review on the Cyber Security. International Journal of Scientific Research and Management, 2021, 9 (12), pp.669-710. ff10.18535/ijsrm/v9i12.ec04ff. ffhal-03509116
- Edwards B, Hofmeyr S, Forrest S. Hype and heavy tails: a closer look at data breaches. J Cyber security 2016;2:3–14.
- Nguyen KD, Rosoff H, Richard SJ. Valuing information security from a phishing attack. In: International Conference on Applied Human Factors and Ergonomics. Cham: Springer, 2017. http://www.pcmag.com/article2/0,2817,2425118,00.asp.
- https://www.eff.org/issues/anonymity.
- http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf.
- https://www.legalserviceindia.com/legal/article-4724-cyber-security-and-cyber-crime-infringes-human-rights-
.html#:~:text=Cyber%20security%20and%20human%20right,liberty%20and%20security%20of%20person.
- http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-openinternet-and-online-freedom-and-opportunity-cyber-security.
- http://www.itu.int/online/termite/index.html
- https://www.freedomonlinecoalition.com/how-we-work/working-groups/workinggroup-1/.
- https://www.gp-digital.org/wp-content/uploads/2015/06/GCCS2015-Webinar-Series-Introductory-Text.pdf