ROOTINDEXING
JOURNAL ABSTRACTING AND INDEXING SERVICE
INTERNATIONAL ADVANCE JOURNAL OF ENGINEERING, SCIENCE AND MANAGEMENT (IAJESM)
July-December 2023, Submitted in September 2023, iajesm2014@gmail.com, ISSN -2393-8048
Multidisciplinary Indexed/Peer Reviewed Journal. SJIF Impact Factor 2023 =6.753

Cyber Law and Technological Advancements: An Overview

Sridhar Pippari, Research Scholar, Glocal School of Technology and Computer Science, Glocal University, Mirzapur, Saharanpu (U.P.)
Dr. Lalit Kumar Khatri, Research Supervisor, Glocal School of Technology and Computer Science, Glocal University, Mirzapur, Saharanpu (U.P.)

Introduction

Cybercrime refers to illegal activities carried out using computers and the Internet. These crimes can range from stealing personal information and financial fraud to hacking and spreading malicious software. Cybercrime poses significant risks to individuals, businesses, and governments worldwide.

Human beings, endowed with unique cognitive abilities, have transformed the world through innovation and adaptation. From basic survival needs to the complexities of modern society, our intellectual prowess has been the driving force behind progress. Initial innovations were driven by survival needs. Human ingenuity has expanded beyond survival to create comforts and luxuries. While innovation has brought immense benefits, it has also led to challenges like climate change and social inequality. As technology advances, ethical considerations become increasingly important. Here are some potential topics:

* The history of a particular invention
* The impact of technology on human relationships
* The ethical dilemmas posed by emerging technologies

A Comprehensive Analysis of Cyber Law and Technological Advancements:

The advent of computers and the internet has drastically altered lifestyles and business operations. A shift from traditional paper-based systems to electronic records and transactions. The rapid pace of technological development outpaces legal frameworks, necessitating constant adaptation. The underlying force driving technological progress and the subsequent legal challenges. The balance between individual privacy and national security in the digital age. Protecting digital content and innovations in the face of rapid dissemination. Ensuring fair practices and consumer protection in online marketplaces.

Internet:

The underlying infrastructure, a vast network of interconnected computers.

A specific service built on top of the internet, using HTML to create and display information. Think of the internet as a highway system. The World Wide Web is like the billboards, signs, and rest stops along that highway. The highway (internet) exists independently, but the billboards (WWW) rely on it to be seen and accessed. For example, we could explore:

- The history of the internet and the WWW
- How the WWW has transformed society
- The technical protocols that underpin both

History of Internet in India:

About the history of the internet in India! Here's a summary of what you shared. The internet was first available in India through ERNET, a research network. Videsh Sanchar Nigam Limited (VSNL) made it commercially available in August 1995. It started with dial-up access in six cities and gradually became a platform for e-commerce. Fibre optic communication accelerated internet growth in the new millennium. Rediff.com, India's first major web portal, launched in 1996. The first cyber cafe and online banking service (by ICICI Bank) followed in 1996 and 1997, respectively

Review of Literature

As many other broad categories of crime, cybercrime too, is a contested concept. There is no consensus regarding the definition of cybercrime, either in the academic literature (e.g., Clough, 2015; Wall, 2007), or in legal and policy documents. As noted in a 2013 review of the UN Office on Drugs and Crime (UNODC, 2013), many of these documents do not even define cybercrime per se, but identify specific acts that constitute cybercrime. To confuse matters further, the terms “computer,” “e-,” “internet,” “digital” and “information crime,” are oft en

used substitutes for cybercrime. Hence, for example, Clough (2015: 9) states that "there are almost as many terms to describe cybercrime as there are cybercrimes."

Monalisa Hati (2016): -

Internet also has its own disadvantages. one in every of the foremost disadvantages is Cybercrime. Cybercrime is outlined as Offences that area unit committed against people or teams of people with a criminal motive to designedly damage the name of the victim or cause physical or mental damage, or loss, to the victim directly or indirectly, victimization fashionable telecommunication networks like net (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS).The provided definition accurately captures the essence of cybercrime as criminal activity conducted through digital means. The cross-border nature of cybercrime is emphasized, underscoring the need for international cooperation. Cybercrime poses significant risks to individuals, businesses, and governments. The ability of cybercriminals to operate anonymously and across borders exacerbates these challenges.

Concept of Cyber Crime

The internet has facilitated a surge in criminal activities, including hacking, piracy, online child exploitation, industrial espionage, and various forms of fraud. Credit card fraud, cyber terrorism, money laundering, and the misuse of secure internet communications pose significant challenges. The entertainment industry is particularly affected by software piracy, while the banking sector faces risks due to vulnerabilities in electronic payment systems.

Understanding the motivations and behaviors of individuals who engage in cybercrime can aid in prevention and detection. The role of international cooperatioGiven the global nature of cybercrime, examining how countries collaborate to combat these threats is essential. Assessing the psychological, social, and economic consequences of cybercrime can inform prevention and response strategies. Analyzing the effectiveness of existing cybersecurity measures and exploring new technologies to combat cybercrime is crucial. Examining the legal framework for addressing cybercrime and the ethical considerations involved in cybersecurity measures is important.

Reasons for Cyber Crimes: -

Both in the physical and digital realms, individuals are susceptible to harm. The necessity of laws to deter and punish unlawful acts is emphasized in both contexts. The acknowledges the difficulties in apprehending and prosecuting cybercriminals due to the borderless nature of the internet. Explore how technological advancements can assist in investigating and prosecuting cybercrimes. Discuss the challenges and opportunities in combating transnational cybercrime through international collaboration. Examine the specific needs of victims of cybercrime and the adequacy of legal protections. Explore how disparities in technological access and literacy can exacerbate the impact of cybercrime on vulnerable populations. the balance between protecting individual privacy and ensuring public safety in the digital age.

Non-Availability or Loss Evidence: -

The shift from physical to digital records has drastically altered the nature of evidence. Gathering and preserving digital evidence is complex due to its volatile and easily altered nature. The internet's inherent anonymity provides a shield for cybercriminals, making it difficult to identify and apprehend them. Cybercriminals often destroy evidence to evade prosecution, further hindering investigations. What advancements in digital forensics are needed to address the challenges of cybercrime investigation? How can law enforcement agencies enhance their capabilities in this area? Given the global nature of cybercrime, what kind of international cooperation is required to effectively combat it? How can countries share digital evidence and intelligence? Are existing legal frameworks sufficient to address cybercrime? What legal challenges arise in prosecuting cybercrimes? How can public awareness about cybercrime prevention be increased? What role can education play in reducing the incidence of cybercrime?

Internet Time Theft: -

Gaining access without permission. The victim incurs costs for internet usage they didn't benefit from. The victim may experience slow internet speeds or service disruptions. This was perhaps one of the first reported cases related to cybercrime in India. However, this case made the police infamous as to their lack of understanding of the nature of cybercrime.

Legal Regulation of Cyber Crime

Clearly outlines the core elements of stalking, both traditional and cyber, emphasizing the intent to cause fear and intimidation. The text highlights the advantages that the internet provides to cybers talkers, such as anonymity and ease of access to personal information. The potential for serious consequences, including physical harm, is correctly emphasized. The text accurately points out that cyberstalking can affect anyone, regardless of gender or relationship to the perpetrator. Defining and prosecuting cyberstalking can be complex due to jurisdictional issues and the evolving nature of technology. Gathering digital evidence is crucial for successful prosecutions, requiring specialized expertise. Providing support and resources to victims of cyberstalking is essential for their recovery.

Child Pornography:

A Heinous Crime, Child pornography is the creation, distribution, or possession of sexually explicit material involving minors. It is a heinous crime that exploits and harms children. Children under the legal age of consent are exploited for sexual gratification. The material depicts children engaged in sexual acts, whether real or simulated. This can include sharing, trading, or selling such material through various means, including the internet. Child pornography has devastating consequences for children: Victims are re-traumatized every time the material is viewed or shared. The demand for child pornography fuels child sexual abuse and trafficking. Children involved in the production of child pornography often suffer severe psychological trauma.

WIPO Internet Copyright Treaty, 1996:

Your points about the origins of WIPO, its key treaties, and its role in addressing internet-related challenges are accurate and informative. The specific challenges faced by intellectual property rights in the digital age. The role of WIPO in addressing these challenges, beyond the internet treaties.

The impact of globalization and technological advancements on intellectual property protection. The controversies surrounding intellectual property rights, such as patent trolls and access to medicines.

The WIPO copyright treaty which was adopted in Geneva on December 20, 1996, and came into force with effect from March 6, 2002, mentions about the right of communication but does not contain a provision on the right of reproduction. It only declares that digital copies will be considered as reproduction for the purpose of copyright law.

Since the issues pertaining to IPR violations on the internet have been dealt with the WIP0 copyright treaty, the member countries are free to develop their own IPR regulations and laws.

Punishment and Prevention to Cyber Crime

Fraudulent Charging of Services.Charging the services used by one person to the account of another through computer manipulation is a cybercrime. This includes unauthorized use of someone else's credit card information or internet hours. Stealing, concealing, destroying, altering, or causing the theft, concealment, destruction, or alteration of computer source code with the intent to cause damage is a cybercrime. This protects the intellectual property of software developers and the integrity of computer systems. These clauses aim to protect consumers and businesses from financial loss and intellectual property theft in the digital realm.

The essential ingredients of section 67 are :

The section covers pornographic websites, magazines, pictures, videos, and all participants in the distribution chain. The section aims to protect society from the harmful effects of obscene content. Defining obscenity can be subjective, leading to difficulties in prosecution. The law must balance the protection of public morality with the right to free expression. The rapid

evolution of technology makes it difficult to regulate online content effectively. The law can have unintended consequences for artists, writers, and filmmakers who may explore mature themes. ISPs face challenges in filtering and blocking obscene content without infringing on privacy rights. Cross-border nature of the internet requires international cooperation to combat online obscenity.

The intent of the sender is immaterial for determining culpability under Section 67. The mere act of transmission is sufficient. Even a single instance of transmission can lead to prosecution. The determination of what constitutes obscene material is based on the specific facts of each case. The law casts a wide net, potentially capturing a broad range of online activities. The potential for overreach and infringement on privacy rights exists. The determination of obscenity is subjective and can vary across cultures and individuals. The law must balance the protection of public morality with the right to freedom of expression. The rapid evolution of technology presents challenges in enforcing the law effectively. Cross-border nature of the internet necessitates international cooperation in combating online obscenity.

Primary organizational cyberattacks

Network devices like routers and firewalls can become overloaded, leading to performance degradation or failure. The increased traffic can cause network congestion, leading to delays and packet loss. As you mentioned, a router between the internet and a local area network (LAN) is a common target or victim of DoS attacks. When subjected to a high volume of attack traffic, the router's resources can be exhausted, resulting in: Slower internet speeds for all users on the LAN. Delays in network communication. Data loss due to network congestion. In severe cases, the router may crash, causing complete network failure. This collateral damage can have significant consequences for businesses, organizations, and individuals reliant on network connectivity.

- **Permanent denial-of-carrier attacks:**

PDoS attacks directly target the hardware itself, rather than software or network resources. Attackers exploit vulnerabilities to replace legitimate firmware with malicious code. The compromised firmware often renders the device unusable. Significant financial loss and operational disruption for victims. PDoS attacks pose a severe threat to critical infrastructure and require robust security measures to prevent and mitigate.

PDoS attacks can be executed rapidly with minimal resources compared to DDoS attacks. The consequences of a successful PDoS attack can be severe, often requiring hardware replacement. Attackers target firmware update mechanisms to deliver malicious code. The development of tools like Phlashdance has increased awareness of PDoS threats. The increasing number of internet-connected devices (IoT) creates a growing attack surface for PDoS attacks.

Conclusion

You've aimed to identify and consolidate different cyberattacks associated with the internet. You're developing a framework to assess, categorize, and address these attacks. Your research seeks to identify limitations in current prevention mechanisms and propose new methods for a more generalized framework. This research is valuable in the ongoing fight against cybercrime. Here are some areas we can delve deeper into: Explore specific cyberattacks like phishing, malware, or botnets, and how your framework can address them. Discuss existing prevention methods like firewalls, intrusion detection systems, and their strengths and weaknesses. Detail the specific characteristics and functionalities of your proposed evaluation framework. The research aims to assess the effectiveness of existing prevention mechanisms. The lack of comprehensive user education is a significant vulnerability. The framework should consider the performance and reliability of prevention measures. Evaluating the cost-effectiveness of different prevention strategies.

Bibliography

1. Tatum, malcolm (2010) “what is a cyber-attack?” Available on-line from: http://www.wisegeek.com/what-is-a-cyberattack.htm

2. Bbc, (2010) "cyber-attacks and terrorism head threats facing uk "available from: http://www.bbc.co.uk/news/uk-11562969
3. Bbc, (2010) "yahoo targeted in china cyber-attacks "available from: http://news.bbc.co.uk/1/hi/8596410.stm
4. Analyzing child victimization on the internet. In f. Schmalleger & m. Pittaro (eds.), crimes of the internet (pp. 28-42). Upper saddle river, nj: pearson education, inc
5. R. Vogt, j. Aycock, and m. J. Jacobson, jr., "armyof botnets," in proceedings of the 2007 network and distributed system security symposium (ndss 2007), pp. 111–123, february2007.
6. Internet security systems. March-2005.
7. "Cyber warfare and the crime of aggression: the need for individual accountability on tomorrow's battlefield"維 Law. duke. edu. Http://www.law.duke.edu/journals/dltr/articles/2010dltr003.html.
8. See, e.g., telephone consumer protection act of 1991, do-not-call implementation act of 2003, can-spam act of 2003
9. Weitzer, Ronald (2003). Current controversies in criminology. Upper saddle river, new jersey: Pearson education press. P. 150.
10. Csonka p. (2000) internet crime; the draft council of Europe convention on cyber-crime: a response to the challenge of crime in the age of the internet? Computer law & security report vol.16 no.5.
11. Geis, g., brown, g. C., &pontell, h. N. (2009). Internet gambling. In f. Schmalleger & m. Pittaro (eds.), crimes of the internet (pp. 417-435). Upper saddle river, nj: pearson education, inc.
12. Gottfredson, m. R., &hirschi, t. (1990). A general theory of crime. Stanford, ca: stanford university press.
13. Cukier, w. &levin, a. (2009). Internet fraud and cybercrime. In f. Schmalleger & m. Pittaro (eds.), crimes of the internet (pp., 251-279). Upper saddle river, nj: pearson education, inc.
14. FBI IC3 (Federal Bureau of Investigation International Crime Complaint Center 2013) "2013 Internet Crime Report"
15. Dr. Ahmad Farroq, 'Cyber Law in India (Law on Internet).' New Era Law Publications, Delhi, 2011.