Title: Cyber Crime and It's Issues and Security in Indian law

Name :- Dr. Om Sharma (Asso. Prof. Harish Chandra P.G College)

Vijaya Jaiswal (Research Scholar)

Institution :- **MAHATMA GANDHI KASHI VIDYAPEETH VARANASI**

Abstract

With over 900 million internet users as of 2023, India ranks among the top countries with the highest number of internet users. The proliferation of internet usage has unfortunately been paralleled by a surge in cybercrimes.[1] Cybercrime has emerged as a significant threat to both individuals and organizations in the digital age. This research paper explores the multifaceted nature of cybercrime, its impacts, and the evolving strategies in cybersecurity.In response to cybersecurity challenges, governments around the world have developed various cybersecurity strategies and policies to protect their cyberspace.[2] By reviewing existing literature, analyzing various types of cybercrimes, and examining notable case studies, it addresses the challenges faced by cybersecurity .This paper provides a comprehensive analysis of India's Cyber Suraksha Raniti 2020, examining its objectives, key components, strengths, and weaknesses.[3] Through a critical evaluation of the policy,professionals and predicts future trends in the field. The findings underscore the importance of continuous innovation and collaborative efforts in combating cybercrime effectively.[4]

Introduction

The National Crime Records Bureau (NCRB) reported a significant increase in cybercrime cases over recent years, highlighting the growing threat.[5] The COVID-19 pandemic accelerated the

1. Internet and Mobile Association of India. (2023). Digital India Report: Internet Usage Statistics.
2. Shoemaker, D., Mead, N. R., & Woody, C. (Eds.). (2021). The Cybersecurity Body of Knowledge. Wiley.
3. Ministry of Electronics and Information Technology, Government of India. (2020). Cyber Suraksha Raniti 2020.
4. Bharati, P. (2019). Cybersecurity Challenges in Developing Nations: The Case of India. Journal of Cyber Policy.

digital shift, leading to increased online transactions and remote work, which cybercriminals exploited.[6]The rapid digitization of information and communication technologies (ICTs) has revolutionized the way we live, work, and interact. While ICTs offer numerous benefits, they also pose significant cybersecurity challenges,Cybercrime encompasses a wide range of illegal activities conducted through the internet, targeting individuals, organizations, and governments. The consequences of cybercrime can be devastating, leading to financial losses, breaches of privacy, and disruptions in critical infrastructure.[7]As the complexity and frequency of cyber-attacks increase, the field of cybersecurity has become more crucial than ever. Cybersecurity involves protecting systems, networks, and data from cyber threats, ensuring the confidentiality, integrity, and availability of information[8] Despite significant advancements in cybersecurity technologies, cybercriminals continue to develop sophisticated methods to bypass defenses, posing a persistent threat to digital security.the Indian government introduced the Cyber Suraksha Raniti 2020 to enhance the country's cybersecurity preparedness andresilience.[9] The purpose of this research paper is to provide an in-depth analysis of cybercrime and security issues, offering insights into the various types of cybercrimes, their impacts, and the measures employed to combat them. Through a comprehensive literature review, the paper will highlight the current state of research, identify gaps, and suggest areas for future investigation. By examining case studies of significant cyber incidents, the paper aims to draw lessons that can inform better security practices. Ultimately, this research seeks to contribute to the ongoing efforts to enhance cybersecurity and mitigate the risks associated with cybercrime[10]

Literature Review - Cybercrime is a rapidly evolving field, necessitating continuous researchand adaptation of security measures. The existing body of literature provides a broad understanding of cybercrime,its implications, and the strategies employed to mitigate its impact. This section reviews key studies and theoretical frameworks that inform our understanding of

---

5. National Crime Records Bureau. (2022). Crime in India 2021: Statistics.
6. Internet and Mobile Association of India. (2023). Digital India Report: Internet Usage Statistics.
7. Wall, D. S. (2007). Cybercrime: The Transformation of Crime in the Information Age. Polity Press.
8. Stallings, W., & Brown, L. (2018). Computer Security: Principles and Practice. Pearson
9. Ministry of ElectIndia. (2020). Cyber Suraksha Raniti 2020.
10. Bharati, P. (2019). Cybersecurity Challenges in Developing Nations: The Case of India. Journal of Cyber Policy.

cybercrime and cybersecurity.Cybercrime has been extensively studied in academic literature, with various scholars addressing its multifaceted nature.Several key sources provide foundational knowledge on the topic:

1. "**Cybercrime: Investigating High-Technology Computer Crime**" by **Robert Moore** (2010) - This book provides a comprehensive overview of different types of cybercrime, investigative techniques, and the challenges faced by law enforcement.[11]

2. "**Cybercrime and Society" by Majid Yar and Kevin F. Steinmetz(2019**) - Yar and Steinmetz offer a sociological perspective on cybercrime, examining its causes, impacts, and the societal responses to this growing threat.[12]

3. "**The Cybersecurity Body of Knowledge" edited by Daniel Shoemaker, Nancy R. Mead, and Carol Woody (2021)** -This collection covers various aspects of cybersecurity, including risk management, legal and ethical issues, and emerging technologies.[13]

Theoretical Frameworks and Models of Cybersecurity-Several theoretical frameworks and models have been developed to understand and mitigate cybercrime:

1. **Routine Activity Theory (RAT)** - Proposed by Cohen and Felson (1979), RAT suggests that cybercrime occurs when a motivated offender, a suitable target, and the absence of a capable guardian converge in time and space. This theory has been adapted to the digital context, emphasizing the importance of cybersecurity measures as capable guardians.[14]

2. **General Deterrence Theory (GDT)** - GDT posits that the fear of punishment can deter individuals from committing crimes. In the context of cybercrime, this theory highlights the need for stringent legal frameworks and effective enforcement to prevent cyber offenses.[15]

3. **The Cybersecurity Capability Maturity Model** - Developed by the U.S.Department of Energy,provides a framework for organizations to assess and improve their cybersecurity capabilities across ten domains,including risk management,incident response and situational awareness[16]

11.Moore,R.(2010).Cybercrime:Investigating High-Technology Computer Crime. Oxford University Press. 12.Yar, M., & Steinmetz, K. F. (2019). Cybercrime and Society. SAGE Publications.

13. Shoemaker, D., Mead, N. R., & Woody,C.(Eds.)(2021). The Cybersecurity Body of Knowledge. Wiley

14.Cohen,L.E.&Felson,M.(1979).Social Change and Crime Rate Trends: A Routine Activity Approach. American Sociological Review, 44(4), 588-608

15.Paternoster, R. (2010). How Much Do We Really Know About Criminal Deterrence? Journal of Criminal Law and Criminology, 100(3), 765-824

Definition and Classification of Cybercrime

Cybercrime encompasses illegal activities conducted via digital devices or networks. It can be broadly classified into the following categories-

1. Hacking -Unauthorized access to computer systems or networks.

Case- 1.Cosmos Bank Hacking Incident (2018) - Description :- One of India's largest cooperative banks, Cosmos Bank, was hacked, resulting in a loss of over INR 94 crore (approximately USD 13 million). Hackers used malware to access the bank's ATM switch server and cloned debit cards to withdraw money from various locations[17].**Impact :** The incident highlighted the vulnerability of banking systems and the need for robust cybersecurity measures in financial institutions**.**[17]

Case- 2.The Flipkart Data Breach (2016) - Hackers gained access to the user database of Flipkart, a leading Indian e-commerce platform, compromising personal information of millions of customers, including names, addresses, and phone numbers.[18] **Impact** The breach raised concerns about the security of e-commerce platforms and the protection of customer data.

2. Phishing- Fraudulent attempts to obtain sensitive information by disguising as a trustworthy entity **Example**:-In 2020, a major phishing scam targeted Indian users by sending emails purportedly from the Income Tax Department, leading victims to fraudulent websites to steal their financial information.[19]

3. Cyberstalking :- Use of the internet to stalk or harass an individual or group

Case- The Kamlesh Tiwari Assassination Case (2019) - Kamlesh Tiwari a Hindu nationalist leader, was assassinated after receiving death threats and being cyberstalked. The attackers used social media to track his movements and plan the attack.[20]**Impact** -This case illustrated the dangers of cyberstalking and the role of social media in facilitating real-world crimes

4. Identity Theft:- Stealing personal information to impersonate someone else.

Case-1.The Aadhar Data Leak (2018) Description An investigation by a news organization

---

16.U.S. Department of Energy. (2014).Cybersecurity Capability Maturity Model (C2M2). Retrieved from https://www.energy.gov/cybersecurity-capability-maturity-model-c2m

17. M. (2018). "Cosmos Bank Hacking Incident: A Case Study."Financial Express

18. "Flipkart Data Breach: Millions of Customers' Data Exposed." (2016). Economic Times

19.Gupta, A. (2020). Phishing Scam Targets Indian Taxpayers. The Times of India.

20.Kamlesh Tiwari Assassination: The Role of Cyberstalking." (2019) India Today

revealed that personal data of millions of Indians[21] **Impact** This incident highlighted significant security flaws in the Aadhaar system and led to calls for stronger data protection regulations

Case 2.The Reliance Jio Data Breach (2017 Description -Personal data of over 120 million customers of Reliance Jio, one of India's largest telecom providers, was leaked online. The breach exposed sensitive information, including names, email addresses, and Aadhaar numbers.[22]

Impact : This incident raised concerns about the security of personal data and the effectiveness of data protection measures in the telecom industry

5. Malware:- Software designed to disrupt, damage, or gain unauthorized access to computer systems.**Example** - The Emotet malware attack in 2019 that infected several Indian companies, disrupting their operations and compromising sensitive data.[23]

6. Ransomware:- Malware that locks users out of their systems until a ransom is paid.

Case - The Andhra Pradesh Power Generation Corporation (APGENCO) Ransomware Attack (2019) -computer systems were infected with ransomware, which encrypted critical data and demanded a ransom for its release. The attack disrupted power generation operations and caused significant financial losses.[24]**Impact**-The attack underscored the importance of cybersecurity in critical infrastructure and the potential risks to national security.

7. Denial-of-Service (DoS) Attacks:- Overloading a network or website to make it unavailable to users **Example** -In 2018, a series of DoS attacks targeted Indian government websites, rendering them inaccessible to the public and disrupting official functions[25]

Case-The Mumbai Power Grid Cyber Attack (2020)- A suspected cyber attack caused a major power outage in Mumbai, affecting millions of residents and halting transportation services

Investigations suggested that Chinese state-sponsored hackers might have targeted the power grid[26]**Impact**: The incident highlighted the vulnerability of critical infrastructure to cyber attacks and the need for enhanced cybersecurity measures to protect national assets

8.Cyber Espionage:-Unauthorized spying to gain access to confidential information.

21.Sharma, R. (2018). "Aadhaar Data Leak: Investigative Report."The Wire

22. Mehta, S. (2017). "Reliance Jio Data Breach: What You Need to Know." **Hindustan Times**.

23.Kumar, R. (2019). Emotet Malware Disrupts Indian Companies. Business Standard

24. "APGENCO Ransomware Attack: An Analysis." (2019). Cybersecurity Magazine.

25.Singh, R. (2018). DoS Attacks Disrupt Indian Government Websites. Economic Times

26."Mumbai Power Grid Cyber Attack: Investigations Point to China." (2020). Times of India

Example-In 2020, it was reported that Chinese hackers conducted cyber espionage against Indian defense and critical infrastructure sectors, aiming to gather sensitive information.[27]

Issues Arising from Cyber Crime in India

1. Economic Impact -Cybercrime has substantial economic consequences. According to a report by the Data Security Council of India (DSCI), the financial losses due to cybercrime are estimated to be in billions of dollars annually. These include direct financial losses from fraud and indirect costs such as loss of productivity and reputational damage.[28]

2. Privacy and Data Security -The increasing number of data breaches has raised significant concerns regarding privacy and data security. High-profile breaches involving sensitive personal information of millions of Indians have led to identity theftand other malicious activities, undermining trust in digital systems[29]

3. Legal and Enforcement Challenges -The transnational nature of cybercrime poses significant challenges for law enforcement. Jurisdictional issues complicate investigations and prosecutions, often necessitating international cooperation. The rapid evolution of cyber threats further strains the capabilities of law enforcement agencies[30]

4. Lack of Awareness and Cyber Hygiene : A considerable portion of the population lacks awareness about cyber threats and the importance of cybersecurity practices.

Poor cyber hygiene, such as using weak passwords and failing to update software, exacerbates vulnerabilities to cyber-attacks.[31]

Cybersecurity Measures in India

1. Preventive Measures : The Indian government has launched various initiatives to bolster cybersecurity. The Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) aims to enhance cyber hygiene by providing tools for malware removal and security best practices.[32]

2. Legal Framework : The primary legislation addressing cybercrime in India is the Information

---

27.Mishra, S. (2020). Chinese Hackers Target Indian Defense Sectors. India Today.

28.. DSCI (2021)Cyber Security in India: A Study on the Economic Impact of Cybercrime.

30 Ramesh, R. (2018). Aadhaar Data Breach Exposes Millions of Indian Citizens.The Guardian

31..Kumar, A. (2020). Cyber Hygiene in India: An Analysis. Journal of Information Security.

32.Ministry of Electronics and Information Technology, Government of India. (2017). Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis

Technology Act, 2000 (IT Act), along with its amendments. This Act provides a legal framework for electronic commerce and digital signatures while criminalizing various cyber offenses[33]

3. Institutional Framework : Several institutions have been established to address cybercrime. The Indian Computer Emergency Response Team (CERT-In) plays a pivotal role in coordinating responses to cybersecurity incidents and enhancing the security of the country's digital infrastructure [34]The National Cyber Security Coordinator (NCSC) oversees the implementation of cybersecurity policies and coordination among different stakeholders[35]

4. International Cooperation : Given the borderless nature of cybercrime, international cooperation is vital. India collaborates with global entities such as INTERPOL and participates in international forums to combat cyber threats. Bilateral agreements with other countries also facilitate information sharing and joint efforts in tackling cybercrime.[36]

Legal Framework for Cybersecurity in India

India's legal framework for addressing cybercrime and ensuring cybersecurity revolves around the Information Technology Act, 2000, and its subsequent amendments. Key aspects of this framework include:-

1. Information Technology Act, 2000 :- This Act is the cornerstone of India's cybersecurity legislation. It defines various cyber offenses and prescribes penalties for them. Key provisions include:

Section 43 :- Penalties for damage to computer systems, including unauthorized access and data theft. Covers offenses such as hacking and identity theft.

Section 67 :- Penalizes the publication or transmission of obscene material in electronic form.

Section 69 :- Grants the government powers to intercept, monitor, and decrypt information to safeguard national security.[37]

2. IT (Amendment) Act, 2008 : This amendment introduced provisions to address emerging cyber threats, including penalties for identity theft, cyberstalking, and cyber terrorism.[38]

33.Digital India. (2020). Cybersecurity Initiatives under Digital India.

34. Information Technology Act, 2000. (2000). Government of India.

35.Indian Computer Emergency Response Team (CERT-In). (2021). Annual Report.

36.National Cyber Security Coordinator (NCSC). (2020). Cybersecurity Policy Implementation Report.

37.: INTERPOL. (2020). International Collaboration in Cybercrime Inv and Information Technology Act,2000. (2000). Government of India, Section 43,67,68

38. IT (Amendment) Act, 2008. Government of India.

3. Personal Data Protection Bill, 2019 : Expected to be enacted soon, this bill aims to provide a comprehensive framework for data protection and privacy, regulating the collection, storage, and processing of personal data, and mandating stringent security measures.[39]

4. Cyber Suraksha Raniti 2020 :-the government introduced the Cyber Suraksha Ranniti 2020 (Cybersecurity Strategy 2020) to strengthen the country's cybersecurity posture and mitigate cyber threats

Objectives of the Cyber Suraksha Raniti 2020:

The Cyber Suraksha Raniti 2020 outlines several key objectives aimed at strengthening India's cybersecurity posture. These objectives include:

1. The policy aims to raise awareness about cybersecurity issues among individuals, businesses, and government agencies.
2. The policy seeks to enhance the cybersecurity infrastructure in India, including the development of secure networks and systems.
3. The policy emphasizes the importance of research and development in cybersecurity and aims to promote innovation in this field.
4. The policy aims to develop a skilled workforce capable of addressing the evolving cybersecurity challenges. [40]

Conclusion

India's rapid digital transformation has brought significant benefits, but it has also exposed the country to substantial cyber threats. The legal and institutional framework in India, centered around the Information Technology Act, 2000, and its amendments, provides a foundation for addressing these challenges. However, several issues, such as jurisdictional challenges, resource constraints, and the evolving nature of cyber threats, require continuous attention and improvement Enhancing public awareness, strengthening legal frameworks, and fostering international cooperation are crucial for effectively combating cybercrime. As India continues to advance its digital infrastructure, ensuring robust cybersecurity measures and addressing the issues arising from cybercrime will be essential for safeguarding its economic and social well-being.

---

39. Personal Data Protection Bill, 2019. (2019). Government of India.

40. Ministry of Electronics and Information Technology, Government of India. (2020). Cyber Suraksha Raniti 2020.