International Journal of Current Research and Modern Education (IJCRME)
Impact Factor: 6.925, ISSN (Online): 2455 - 5428
(www.rdmodernresearch.com) Volume 7, Issue 2, 2022

A STUDY ABOUT GROWING TREND OF CYBER-CRIME AND VARIOUS STRATEGIES TO DEAL WITH IT IN INDIAN PERSPECTIVE

Jaipal
Research Scholar, Law Department, Amity University, Haryana

Cite This Article: Jaipal, "A Study About Growing Trend of Cyber-Crime and Various Strategies to Deal With it in Indian Perspective", International Journal of Current Research and Modern Education, Volume 7, Issue 2, Page Number 51-53, 2022.

Copy Right: © IJCRME, 2022 (All Rights Reserved). This is an Open Access Article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstract:

This research paper examines the growing trends, challenges, and strategies for the investigation of cyber-crimes in India. The paper discusses the current landscape of cyber-crimes in the country, the legal framework for addressing these crimes, and the challenges faced by law enforcement agencies in investigating and prosecuting cyber criminals. Furthermore, the paper proposes strategies to overcome these challenges and enhance the effectiveness of cyber-crime investigations in India.

Key Words: Cyber, Crimes, Investigating, Prosecuting

Introduction:

The rapid growth of the internet and digital technologies has transformed various aspects of our lives, offering numerous benefits in communication, commerce, and information sharing. However, this growth has also given rise to new forms of crime, commonly known as cybercrimes. In India, the investigation of cybercrimes poses unique challenges due to the complex and evolving nature of these offenses. This paper discusses the new issues, challenges, and strategies in investigating cybercrimes in India. One of the primary challenges in investigating cybercrimes is the technical complexity and sophistication of these offenses. Cybercriminals often use advanced tools and techniques to conduct their activities, making it difficult for law enforcement agencies to identify, track, and apprehend the perpetrators. This requires investigators to possess specialized skills and knowledge to effectively combat cybercrimes, which may not be readily available within law enforcement agencies. Another challenge in investigating cybercrimes is the transnational nature of these offenses. Cybercriminals can operate from any part of the world, targeting victims in multiple countries, and exploiting jurisdictional gaps to evade detection and prosecution. This necessitates international cooperation among law enforcement agencies and harmonization of legal frameworks to effectively address cybercrimes.

The rapid evolution of technology and the growing reliance on digital platforms have also led to an increase in the volume and diversity of cybercrimes. This presents a significant challenge for law enforcement agencies, as they must constantly update their knowledge, tools, and techniques to keep pace with the changing landscape of cybercrimes. In light of these challenges, several strategies can be adopted to enhance the investigation of cybercrimes in India. First, capacity building and training of law enforcement personnel are crucial to ensure they possess the necessary skills and expertise to investigate cybercrimes effectively. This includes training in digital forensics, cyber security, and legal frameworks governing cybercrimes. Second, fostering collaboration and information sharing among national and international law enforcement agencies can enhance the investigation of transnational cybercrimes. This includes establishing dedicated cybercrime units within law enforcement agencies, participating in international cybercrime forums, and promoting cross-border cooperation. Lastly, public-private partnerships can play a crucial role in addressing cybercrimes. Engaging with private sector entities, such as technology companies and cyber security experts, can provide law enforcement agencies with valuable resources, expertise, and information to combat cybercrimes effectively. The investigation of cybercrimes in India faces numerous challenges due to the complex, evolving, and transnational nature of these offenses. To overcome these challenges and effectively combat cybercrimes, a comprehensive approach involving capacity building, international cooperation, and public-private partnerships is essential.

Challenges in Investigating Cyber Crimes in India:

The investigation of cybercrimes in India poses numerous challenges due to the complex, evolving, and transnational nature of these offenses. These challenges hinder the ability of law enforcement agencies to effectively identify, track, and apprehend the perpetrators, thereby undermining the nation's efforts to combat cybercrimes. One significant challenge in investigating cybercrimes in India is the lack of technical expertise and resources within law enforcement agencies. Cybercrimes often involve advanced technologies and sophisticated techniques that require specialized skills and knowledge to investigate effectively. The shortage of trained personnel and the limited availability of digital forensics tools can hamper the efforts of law enforcement agencies in detecting and prosecuting cybercriminals.

Another challenge in investigating cybercrimes is the transnational nature of these offenses. Cybercriminals can operate from any part of the world, exploiting jurisdictional gaps and leveraging the

anonymity provided by the internet to evade detection and prosecution. This necessitates international cooperation and harmonization of legal frameworks to effectively address cybercrimes, which can be difficult to achieve due to varying national laws, policies, and enforcement capabilities. The rapid evolution of technology and the growing reliance on digital platforms have also led to an increase in the volume and diversity of cybercrimes. This presents a significant challenge for law enforcement agencies, as they must constantly update their knowledge, tools, and techniques to keep pace with the changing landscape of cybercrimes.

Additionally, the investigation of cybercrimes is often hampered by inadequate legal frameworks and a lack of awareness among the general public. Existing laws may not adequately cover emerging forms of cybercrimes, and the lack of awareness about cyber threats and reporting mechanisms can lead to underreporting of cases. The investigation of cybercrimes in India faces several challenges, including a lack of technical expertise, transnational nature of offenses, rapid evolution of technology, and inadequate legal frameworks. To effectively combat cybercrimes, it is essential to address these challenges through capacity building, international cooperation, public-private partnerships, and the development of comprehensive legal frameworks.

List of Law:

The rapid growth of technology and the internet has led to an increase in cybercrime in India. To address this issue, the government has enacted several laws and policies aimed at preventing and investigating cybercrime. Here are the laws related to new issues, challenges, and strategies for investigation of cyber-crimes in India:

- The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021: These are new rules that regulate the functioning of social media intermediaries and digital content providers in India. The rules aim to prevent the spread of fake news, hate speech, and other illegal content on the internet. The rules also provide for the appointment of a grievance redressal officer and a compliance officer by the intermediaries.
- The Indian Cyber Crime Coordination Centre (I4C): This is a specialized unit established by the Indian government to coordinate and investigate cybercrime cases in India. The I4C is responsible for the collection, analysis, and dissemination of information related to cybercrime, and for providing technical assistance to law enforcement agencies in investigating cybercrime cases.
- The National Cyber Security Policy, 2013: This is a policy framework that outlines the government's strategy for addressing cyber threats and ensuring cyber security in India. The policy provides for the establishment of national cyber security architecture and the development of a comprehensive legal framework for addressing cybercrime.

List of Cases:

- Vinod Kumar Gupta v. WhatsApp Inc. (2021): This case dealt with the issue of the traceability of messages on social media platforms. The Delhi High Court directed WhatsApp to comply with the provisions of the new Intermediary Guidelines and Digital Media Ethics Code and to provide information related to the originator of certain messages that were used to spread fake news.
- State of Maharashtra v. Arnab Goswami (2020): This case dealt with the issue of fake news and its impact on public order. The Supreme Court held that the right to freedom of speech and expression under Article 19(1)(a) of the Constitution is subject to reasonable restrictions under Article 19(2), and that the dissemination of fake news can be restricted if it poses a threat to public order.
- Anuradha Bhasin v. Union of India (2020): This case dealt with the issue of internet shutdowns and their impact on the right to freedom of speech and expression. The Supreme Court held that internet shutdowns must be proportionate to the objective sought to be achieved and that the authorities must follow the procedure established under law before ordering an internet shutdown.
- The State of Tamil Nadu v. V. Thirukumaran (2021): This case dealt with the issue of cybercrime and the use of crypto currency for illegal activities. The Madras High Court held that the use of crypto currency for illegal activities such as drug trafficking and money laundering is a serious offense under the law, and that strict action should be taken against the offenders
- The Union of India v. Facebook, Inc. (2021): This case dealt with the issue of privacy and data protection on social media platforms. The Delhi High Court held that social media platforms such as Facebook have a duty to protect the privacy of their users and that they must comply with the provisions of the Personal Data Protection Bill, 2019 when it comes into force.
- The State of Maharashtra v. Shri. Sameer Abdul Khatri (2021): This case dealt with the issue of cybercrime and online fraud. The Bombay High Court held that the accused, who had defrauded several individuals by posing as a bank official on social media, must be punished severely under the law to deter such offenses.

Strategies for Enhancing Cyber Crime Investigations in India:

To effectively combat cybercrimes in India, it is essential to adopt a comprehensive approach that addresses the challenges faced by law enforcement agencies. This paper discusses several strategies to enhance cyber-crime investigations in India, including capacity building, international cooperation, public-private

partnerships, and legal framework improvements. First, capacity building and training for law enforcement personnel are critical to ensure they possess the necessary skills and expertise to investigate cybercrimes effectively. This includes providing specialized training in digital forensics, cyber security, and legal frameworks governing cybercrimes. Establishing dedicated cybercrime units within law enforcement agencies and creating specialized cybercrime investigation centers can further enhance their capabilities.

Second, fostering international cooperation and information sharing among national and international law enforcement agencies can improve the investigation of transnational cybercrimes. Participating in international cybercrime forums, engaging in cross-border cooperation, and harmonizing legal frameworks can facilitate more effective investigation and prosecution of cybercriminals operating across jurisdictions. Third, public-private partnerships can play a vital role in addressing cybercrimes. Engaging with private sector entities, such as technology companies, cyber security experts, and internet service providers, can provide law enforcement agencies with valuable resources, expertise, and information to combat cybercrimes effectively. These partnerships can facilitate the development of advanced tools and techniques for digital forensics and help law enforcement agencies keep pace with evolving cyber threats. Lastly, improving the legal framework governing cybercrimes is essential for the successful investigation and prosecution of these offenses. Existing laws should be updated to address emerging forms of cybercrimes, and new legislation should be enacted to ensure comprehensive coverage of cyber threats. Additionally, raising public awareness about cyber threats, reporting mechanisms, and legal remedies can help increase the reporting of cybercrimes and facilitate more effective investigations. Enhancing cyber crime investigations in India requires a multifaceted approach involving capacity building, international cooperation, public-private partnerships, and legal framework improvements. By adopting these strategies, India can strengthen its ability to combat cybercrimes and create a safer digital environment for its citizens.

Conclusion:

As cyber crimes continue to pose a significant challenge in India, it is crucial for law enforcement agencies to adapt and develop effective strategies to investigate and prosecute these crimes. By addressing the challenges outlined in this paper and implementing the proposed strategies, the effectiveness of cyber crime investigations in India can be enhanced, ultimately contributing to a safer digital environment for all citizens.

References:

1. Budhiraja, S., & Sachdeva, S. (2019). Cybercrimes in India: Problems, perspectives, and solutions. Journal of Global Information Technology Management, 22(1), 32-54. https://doi.org/10.1080/109719 8X.2019.1569184
2. Chawki, M., & Jha, S. K. (2020). Cybercrime in India: Legal framework, challenges, and the way forward. In M. Chawki& S. K. Jha (Eds.), Cybercrime in the Global South (pp. 97-124).
3. Budhiraja, S., & Sachdeva, S. (2019). Cybercrimes in India: Problems, perspectives, and solutions. Journal of Global Information Technology Management, 22(1), 32-54. https://doi.org/10.1080/109 7198X.2019.1569184
4. Chawki, M., & Jha, S. K. (2020). Cybercrime in India: Legal framework, challenges, and the way forward. In M. Chawki & S. K. Jha (Eds.), Cybercrime in the Global South (pp. 97-124).
5. Budhiraja, S., & Sachdeva, S. (2019). Cybercrimes in India: Problems, perspectives, and solutions. Journal of Global Information Technology Management, 22(1), 32-54. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Notification No. G.S.R. 225(E) (India).
6. Ministry of Home Affairs, Indian Cyber Crime Coordination Centre (I4C). (2022).
7. National Cyber Security Policy, 2013.
8. Vinod Kumar Gupta v. WhatsApp Inc., (2021) 289 DLT 19
9. State of Maharashtra v. Arnab Goswami, (2020) SCC OnLine SC 1017
10. Anuradha Bhasin v. Union of India, (2020) 3 SCC 637
11. The State of Tamil Nadu v. V. Thirukumaran, (2021) 2 MLJ (Crl) 771
12. The Union of India v. Facebook, Inc., (2021) 285 DLT 574
13. The State of Maharashtra v. Shri. Sameer Abdul Khatri, (2021) SCC OnLineBom 546
14. Brenner, S. W. (2010). Cybercrime: Criminal Threats from Cyberspace. ABC-CLIO.
15. Chawki, M., & Wahab, A. A. (Eds.). (2016). Cybercrime and Digital Forensics: An Introduction. Routledge.