Journal of Namibian Studies, 35 S1 (2023) : 5568-5576 ISSN: 2197-5523 (online)

The Role Of Police In Combating Cybercrime Within The Legal Framework Of India

Jaswant Singh[1] & Haider Ali[2]

Institute of Legal Studies & Research
Mangalayatan University, Aligarh -202146, Uttar Pradesh, India
E-mails: jaswant.singh@ mangalayatan.edu.in, haider.ali@mangalayatan.edu.in

ABSTRACT

The rise of cybercrime has fundamentally altered our understanding of the term "space" in relation to crime. We can no longer view crime and criminality solely through a geographical lens. Cybercrime defies traditional borders, often extending beyond physical limitations. While advancements in Information and Communication Technology (ICT) have greatly benefited society, they have also facilitated a variety of illicit activities conducted online, such as hacking, identity theft, online fraud, cyberbullying, & cyber terrorism. These activities present significant challenges as they utilize sophisticated technological tools to exploit vulnerabilities.

In India, the widespread availability of internet access and the rapid digitization of services have made the nation particularly appealing to cybercriminals, who take advantage of weaknesses in networks, systems, and the naivety of users. As one of the world's largest and fastest-growing digital economies, India is especially at risk from cyber terrorism. Consequently, cybercrime is increasingly recognized as a major societal challenge, prompting a critical need for governments to take decisive action. In response, various legislative measures and institutional frameworks have been established to tackle the complexities of the cyber realm. Nonetheless, due to the ever-evolving nature of cyberspace, there is an urgent need for enhanced cyber policing and thorough investigations into cybercrime.

The primary aims of my research paper are to explore how police can be effectively regulated in their efforts to combat cybercrime, to gain insights into the nature of cyber policing and its inherent challenges, to examine theoretical models of cyber-crime investigation, and to discuss various issues and obstacles faced in cyber policing & cyber-crime investigation.

Keywords: Transcending, Geographical, Boundaries, Mechanism, Information and Communication Technology.

INTRODUCTION

The emergence of cybercrime has fundamentally altered the concept of 'space' within the realm of criminal activity. We can no longer limit our understanding of crime to geographical parameters; instead, cybercrime operates beyond physical borders, defying traditional definitions. While advancements in ICT have brought numerous benefits to society, they have also facilitated a spectrum of illicit activities conducted online, such as hacking, identity theft, online fraud, cyberbullying, & cyber terrorism. These developments present both significant challenges and opportunities, as they employ sophisticated technological tools for criminal purposes.

The widespread availability of internet access and the swift digitization of services have made India an appealing target for cybercriminals, who take advantage of vulnerabilities in networks, systems, and unsuspecting individuals. As one of the largest and fastest-growing digital economies globally, India is particularly susceptible to threats from cyber terrorism. Consequently, there is an increasing recognition of cybercrime as a major societal issue, highlighting the urgent need for governments to respond effectively. In response, many governments have enacted legislation and set up institutional frameworks to tackle the complexities of the cyber landscape. Nevertheless, given the rapidly evolving nature of cyberspace, there remains an urgent need for enhanced cyber policing and more robust investigations into cybercrime.[1]

NATURE OF CYBER POLICING

When cyber-crimes occur, law enforcement agencies bear the responsibility of investigating these incidents and apprehending those responsible. This responsibility often falls to specialized cyber-crime units within police departments, commonly referred to as cyber police.[2]

[1] Charles Chatterjee & Anna Lefcovitch, *Cyber Security*, *Diplomacy and International Law*, 108 AMICUS CURIAE 2 (2016).

[2] Emeka C. Adibe, Ndubuisi Nwafor & Chibuike Amaucheazi, *Information Technology*, *Terrorism Financing and*

Key considerations regarding cyber policing include:

- What defines the role of cyber policing?
- Can public law enforcement effectively address the challenges posed by cyber-crime on its own?
- Is it feasible for cyber policing to manage these threats independently?
- Should private corporations or non-governmental organizations (NGOs) be involved to achieve more effective outcomes?

The IT Act aims to provide answers to these questions by establishing a legislative framework for cyber policing in India through its various provisions. For instance, Section 69[3] empowers the government or designated agencies to intercept, monitor, or decrypt information generated, transmitted, received, or stored within computer resources, provided that procedures outlined in the section are followed. This authority can be exercised if Central or State Government determines it is necessary to protect sovereignty & integrity of India, national defense, state security, friendly relations with foreign nations, public order, or to prevent incitement to any cognizable offense related to these areas or for the investigation of any crime.

In such instances, prescribed procedures must be adhered to, and the rationale for such actions must be documented by the appropriate government agency. Additionally, intermediaries are required to provide technical assistance and facilities when requested. This assistance can include:

- Granting access to computer resources containing relevant information.
- Facilitating the interception, monitoring, or decryption of information as necessary.
- Supplying information stored in computer resources.

Failure to comply with these requirements can result in imprisonment for up to seven years and the imposition of fines.

Financial Institution's Role in Combating Terrorism, 2 IRLJ 29 (May 2020).

[3] Information Technology Act, 2000, § 69 (2000).

Section 69A of IT Act, 2000,[4] gives Central Government or its officials authority to block public access to certain information via computer resources. Meanwhile, Section 69B discusses power to authorize monitoring & collection of traffic data through computer resources to bolster cybersecurity. Central Government can notify any government agency to collect traffic data generated, transmitted, received, or stored within computer resources, aiming to enhance cyber security & to identify, analyze, and prevent the spread of intrusions or computer viruses within country.

Traditionally, responsibility for monitoring the cyber landscape has been viewed as falling solely to public law enforcement. However, academic discussions suggest that monitoring can also be effectively carried out by corporate security forces and NGOs. The effectiveness of cyber policing will hinge on fostering collaboration among public police, corporate entities, and non-governmental organizations. The task of policing cyberspace is becoming increasingly challenging due to the high mobility of cyber criminals.

COORDINATION/INTERNATIONALPROTOCOLSAMONG COUNTRIES

Criminal investigations in cyberspace present unique challenges that differ significantly from those in the physical world. The virtual environment eliminates traditional barriers, fosters anonymity, and creates geographical detachment, which necessitates a reevaluation of crime and its perpetrators. In this digital realm, a criminal and their victim may exist in entirely different locations, often lacking any direct connection. Consequently, investigative processes must navigate not only the laws of individual states but, in some instances, the legal frameworks of multiple countries. This complexity underscores the need for enhanced understanding, collaboration, and coordination among legal authorities across various jurisdictions.

To address these challenges on an international scale, Budapest Convention on Cybercrime was established as first treaty aimed at tackling internet & computer-related offenses.[5] This convention seeks to harmonize national laws, improve investigative methodologies, and foster greater cooperation between nations. It officially took effect on July 1, 2004. However, the convention has yet to gain widespread acceptance, with several countries,

[4] Information Technology Act, No. 21 of 2000, § 69A (2000).
[5] European Treaty Series - No. 185, Convention on Cybercrime, Nov. 23, 2001.

including India, opting not to ratify it due to concerns over national sovereignty and its absence from initial drafts.

CYBER CRIME INVESTIGATION

Cybercrime units are tasked with investigating incidents of cybercrime and apprehending those responsible. They utilize specialized teams equipped with advanced skills and technologies to gather evidence, trace digital activities, and initiate legal proceedings. O Ciarduain identifies a framework known as the 'Extended Model of Cybercrime Investigation,'[6] which includes thirteen critical activities outlined below:

- Awareness – recognizing the need for an investigation.
- Authorisation – acquiring legal permission, such as a warrant.
- Planning – utilizing the information collected by investigator.
- Notification – alerting subjects & relevant parties that investigation is underway.
- Search & Identification of Evidence – locating devices, such as computers used by suspects.
- Collection of Evidence – securing potential evidence for further examination.
- Transportation of Evidence – moving evidence to designated location for analysis.
- Storage of Evidence – ensuring that storage practices minimize the risk of contamination.
- Examination of Evidence – employing specialized techniques to recover deleted data.
- Hypothesis – developing a provisional explanation of the events.
- Presentation of the Hypothesis – communicating findings to a jury or other relevant parties.

[6] Ó Ciardhuáin, Séamus. "An Extended Model of Cybercrime Investigations." *International Journal of Digital Evidence* 3 (2004).

- Proof/Defense of the Hypothesis – considering alternative explanations and counterarguments.

- Dissemination of Information – sharing insights that may inform future investigations.

Understanding the cybercrime investigation process in India is essential for this module. According to Sec. 78 of Act, 2008,[7] authority to investigate cybercrimes is specified, stating, "Notwithstanding anything contained in Cr.P.C., 1973, no police officer below rank of Inspector shall investigate any offence."

Sec. 80 grants police officers & authorized personnel the power to enter and search premises without a warrant. It specifies that officers of a certain rank may apprehend individuals reasonably suspected of committing, attempting to commit, or being in act of committing an offence. Furthermore, Sec. 80(2) states that if a person is arrested by officer other than police officer, they must be presented before Magistrate or officer in charge of police station without unnecessary delay.

The challenges faced in cybercrime investigations are primarily due to jurisdictional limitations, ambiguities in the law, and a lack of understanding of technology-based crimes among key stakeholders in the criminal justice system. Many states operate with only one or a handful of specialized cybercrime units, which are often overwhelmed by the rapid increase in cyber offenses. Victims frequently encounter difficulties in accessing the appropriate police stations to file their complaints. The major obstacles in cybercrime investigations include:

- A shortage of trained cyber investigators.

- Limited availability of cyber forensic facilities in forensic laboratories.

- Delays in obtaining forensic reports due to significant backlogs.

- Insufficient institutional mechanisms for accessing expertise from the cyber industry.

The effectiveness of law enforcement in cyber policing and investigation fundamentally hinges on the capacity of these units. The skill set of personnel assigned to cybercrime investigation units is crucial for operational success. Existing recruitment standards for police in India may not adequately address the

[7] Information Technology (Amendment) Act, No. 10 of 2009, § 78 (India).

unique demands of this field. Therefore, it is imperative for Indian law enforcement agencies to attract and employ top talent in cyber technology to effectively combat the evolving threats posed by sophisticated cybercriminals.

LEGAL FRAMEWORK OF CYBER LAW

Domain of cyber policing & cyber-crime investigation is characterized by rapidly evolving landscape, presenting numerous challenges that require attention. A primary concern within this realm is the legal framework governing cyber activities. In India, prior to implementation of IT Act, 2000, cyber landscape was largely unregulated, leading to considerable uncertainty among law enforcement regarding the handling of crimes committed online. The introduction of the IT Act marked a significant turning point, as it provided a legal foundation for defining cyber-crime and establishing procedures for cyber policing and investigations.[8]

Recognizing the need for adaptability in response to the dynamic nature of cyber-crime, amendments were made to the Act in 2008. These revisions expanded the scope of cyber-crimes to include offenses such as child pornography and cyber terrorism, while also shifting investigative authority from the Deputy Superintendent of Police to Inspectors. This evolution raises critical questions that the legal framework must address, including:

- What constitutes cyber-crime?
- What procedures are to be followed in investigating cyber-crimes?
- What penalties will apply to individuals convicted of such crimes?
- How is evidence defined within the context of cyberspace?

Effective legal frameworks are crucial for prosecuting cyber criminals and deterring potential offenders. In India, various laws, including the IT Act, 2000 and its subsequent amendments, have been enacted to tackle different facets of cyber-crime. The police play a vital role in enforcing these laws and delivering justice, working to ensure that the legal infrastructure is sufficient for the prosecution of cyber criminals. Notably, the IT (Amendment) Act, 2008, grants police officer's specific powers to investigate cyber-

[8] Scott J. Shackelford, *Inside the Drive for Cyber Peace: Unpacking Implications for Practitioners and Policymakers*, 21 U.C. DAVIS BUS. L.J. 285 (Spring 2021).

crimes, including the authority to conduct searches and make arrests without a warrant.

LANDMARK JUDGEMENT OF SUPREME COURT

In Prakash Singh & Ors. v. Union of India & Ors.,[9] court included a significant directive: it advocated for the separation of investigative police from those responsible for maintaining law and order. This separation aims to enhance the efficiency of investigations, improve expertise, and foster better relationships with the community. The need for cooperation between these two branches was also stressed. This principle has been reiterated in the Model Police Act, 2006, with several state legislatures adopting these recommendations verbatim.

The underlying implication is that law enforcement personnel require specialized training, particularly given the complexities of contemporary crime, including cybercrime, which necessitates advanced investigative skills. This calls for the recruitment and training of dedicated personnel to address these challenges effectively, ensuring they can develop their expertise over time. Additionally, it is noteworthy that court previously invalidated Section 66A, deeming it unconstitutional. This provision was criticized for being excessively restrictive and for leading to the detention of individuals for sharing content deemed objectionable.[10]

CONCLUSION

Contemporary landscape of cyberspace poses significant challenges for criminology, police science, law enforcement, & policing. In India, combating cybercrime has become a persistent challenge that necessitates a collaborative approach among law enforcement agencies, governmental entities, the private sector, and the general public. Since the 1990s, cyberspace has developed into a significant domain for criminal activities, fundamentally altering the nature and breadth of crime and victimization. This evolution has given rise to the field of cyber criminology, which investigates the motivations behind crimes committed in digital environments and their repercussions in the physical world.

To effectively counter cyber threats, it is essential for Indian law enforcement to be equipped with adequate resources and specialized knowledge. An adaptable legislative framework is crucial and must be periodically updated to address emerging challenges. Additionally, a robust national cybersecurity strategy is

[9] Writ Petition (Civil) 310 of 1996.
[10] *Shreya Singhal v. Union of India*, AIR 2015 SC 1523.

vital for ensuring a secure and resilient digital environment for citizens, businesses, and governmental operations. This cybersecurity framework delineates vision, objectives, guiding principles, & methodologies necessary to achieve cybersecurity goals.

Furthermore, developing comprehensive modules for cybercrime investigations, training cybercrime investigators in both investigation techniques and forensics, and ensuring the availability of essential equipment through state forensic science laboratories are critical components for effective cybercrime policing. Hence, the current landscape of cyber policing and investigation demands heightened professionalism, enhanced confidentiality, increased reliance on automated technologies, and a nuanced understanding of the complexities inherent in the digital realm.

References:

1. Information Technology (Amendment) Act, No. 10 of 2009, India.
2. Emeka C. Adibe, Ndubuisi Nwafor & Chibuike Amaucheazi, Information Technology, Terrorism Financing and Financial Institution's Role in Combating Terrorism, 2 IRLJ 29 (May 2020).
3. Emeka C. Adibe, Ndubuisi Nwafor & Chibuike Amaucheazi, Information Technology, Terrorism Financing and Financial Institution's Role in Combating Terrorism, 2 IRLJ 29 (May 2020).
4. Scott J. Shackelford, Inside the Drive for Cyber Peace: Unpacking Implications for Practitioners and Policymakers, 21 U.C. DAVIS BUS. L.J. 285 (Spring 2021).