Bureaucratic Challenges in Cybercrime Prevention: The Case of West Bengal Police

SAYANTAN SAHA

PhD Research Scholar

Department of Political Science

University of Kalyani

Abstract -

The West Bengal police bureaucracy confronts a variety of challenges in addressing today's technology-related crimes. The increase in cyber threats necessitates updating the police force with modern policing methods, as traditional methods often fail to tackle today's sophisticated and frequent cybercrime cases. This paper focuses on cybercrime policing, with the option of offering solutions to the various aspects involved. The study is qualitative, and the researcher conducted interviews with both male and female police officers of different ranks from different divisions of cybercrime police stations in West Bengal. Focus group discussions were done to gather more diverse information; after this analysis, several research findings highlighted several critical issues: low levels of preparedness in terms of digital investigation training, absence or inadequate equipment, and the current threat landscape that is constantly changing and often surpassing the police's readiness. Red tape also prevents critical decision-making processes and collaboration between departments, which exacerbates the problem of cybercrime.

Keywords - Cyber Crime,Cybercrime Policing,West Bengal,Challenges,Digital Forensics

Introduction

West Bengal is now a prime target for criminals as more businesses and government-related areas turn into online enterprises, ranging from banking institutions, online shopping, governance, and education. Unfortunately, as the state advances and increases its use of technology, it also becomes more vulnerable to cyber risks such as hacking, phishing, data leaks, and ransomware attacks. These challenges necessitate the establishment of additional government institutions and bureaucracies. However, it is rather challenging to prevent cybercrime in West Bengal due to bureaucratic factors that may slow down the efficiency of cybersecurity. With high population density and the increasing rate of digitization, weak cyber security measures and the appearance of IT cities beckon cyber criminals, which has made West Bengal a hub for cyber crimes (A Deep Dive into Cybercrime Trends IMPACTING India, n.d.). The state's diverse economy, encompassing the finance and healthcare sectors, presents well-defined targets for potential attacks.

Meaning and Definition of Cybercrime

Cybercrime, also known as computer-related crime, can be defined as any criminal activity that employs a computer, network, or any form of computer devices for unlawful deeds (Cybercrime.org.za, n. d.). In recent years, the expansion of the internet and digital technology has led to an increase in cybercrime. The scope of these misdemeanors has expanded to include unauthorized access to computer systems and data, identity theft, fraud, stalking, and content piracy. Such activities affect not only the immediate victims but also business organizations, governments, and even the security systems of a given geographical region. Cybercrime is not a singular phenomenon; it consists of different forms that differ in their features and consequences. The most popular categories are financial crimes, where cyber attackers employ phishing, online banking fraud, and credit card fraud with the aim of robbing people and companies of money. Another significant category is the use of malware to steal classified information for espionage, and most often, the targets are governments, companies, or military organizations. Furthermore, cyberbullying and harassment entail sending or posting threats, menaces, or otherwise negatively affecting people using computers and telecommunication networks, and this tends to have adverse impacts on the psychological well-being of the recipients. Finally, the terms hacking and malware refer to the unauthorized access and control of computer systems, resulting in data theft, system sabotage, or financial loss (Vadza, 2011).

Role of Law Enforcement Agencies to prevent cybercrime

The police department plays a central role in combating cybercrime, as people who have been victims of such crimes should visit the nearest cyber police station and report in writing. Based on the concerns raised by the public, the police strive to apprehend these cybercriminals and secure justice for the victims (The Indian Express, 2023). The police encounter numerous challenges while fighting cybercrime. The dynamic nature of cybercrime poses a continuing challenge for law enforcement agencies as they attempt to tackle it. The absence of enough police officers in police stations causes a delay in the detection of cybercriminals, resulting in inadequate infrastructure in cyber police stations. The fight against cybercrime requires advanced technology, which police stations do not have (Harkin, Whelan, & Chang, 2018). Additionally, police officers must be proficient in using the latest tools and machinery to combat cybercrime, but proper training is lacking in cyber police stations. In West Bengal, there are still 34 cybercrime police stations (West Bengal Police, n.d.).

Cybercrime in West Bengal

Cybercrime in West Bengal has also recently increased due to various socio-economic and technological factors. The overall advancement of digital technology, especially in the current state after the COVID-19 pandemic, includes financial transactions, communication, and even purchasing any item through digital platforms. While this has boosted the region in a number of ways, it has also led to a high vulnerability to cyber theft. Regrettably, a significant portion of West Bengal's population, particularly those living in rural and semi-urban areas, lacks knowledge about safe internet practices, making them vulnerable to cybercriminals. Further, West Bengal being on the borders of an international territory puts it at a higher risk of cross-border cybercrime, which adds to the problems of investigation and prosecution of this crime. However, the fact that criminals constantly innovate and devise new methods to perpetrate their crimes, while the police and other security organizations typically implement preventive measures, exacerbates the challenge they face. Observing the current trend of computer crime, the West Bengal Police have gained an understanding of this emerging trend. They also diagnose and study cybercrimes, trace the origins of cyberattacks with digital forensics, and gather information about the offenders. Another element of the police's approach is awareness-raising, which envisages organizing information campaigns to inform the population about the dangers associated with cybercrime and the need to protect themselves against such threats. It is essential for interconnection here, as cybercrime necessarily transcends state and national jurisdictions. Furthermore, the police force prioritizes the professional development of its human capital, which includes keeping them updated on the latest trends in cybercrimes and their prevention strategies.

The statistics on cybercrime cases recorded in several West Bengal police districts for 2022 show notable differences in the prevalence and recording of such crimes. Kolkata, with 75 instances, is the leader in cybercrime registrations, followed by Purba Medinipur (34), Barrackpur PC (27), Asansol-Durgapur PC (25), and Siligiri PC (23). Other districts—Darjeeling, Howrah GRP, Kharagpur GRP, Purulia, Sealdah GRP, and Ranaghat—recorded zero incidents, implying either a reduced frequency of cybercrime or underreporting. Many districts—including Bankura, Baruipur, and Murshidabad—recorded less than 10 incidents, suggesting possible geographical differences in cybercrime activity and police responsiveness. Reflecting the increasing difficulty presented by cyberthreats in both urban and rural areas, West Bengal's overall number of cybercrime cases came in at 401 for the year. These differences could also point to different degrees of digital literacy, awareness, and tools at hand for law enforcement around the districts.(Source NCRB 2022 Data)

Literature Review

Tatiana Tropina's (2009) article, "Cyber-policing: The article "Role of the Police in Fighting Cybercrime," states the problems that police organizations encounter when it comes to managing new threats in cyberspace and the need to have good substantive criminal legislation and procedural techniques in handling cybercrimes. It looks at the policing of cybercrime and underscores the use of technology, capacity, and multi-stakeholder collaboration in addressing cybercrime as critical improvements. It stresses the need for the pursuit of traditional measures toward policing, the adoption of new reforms and legal tools for enforcement of the law, and skills in handling materials with electronic proof. The study also calls for more forensic software development, such as Microsoft's COFEE software, that can help the police in investigations. The article does not compare the views with other interested parties, including law enforcement, cybercrime specialists, and non-governmental organizations, which could give a better understanding of the role and tasks of law enforcement in combating cybercrime. This paper does not comprehensively discuss the fine details of appropriate legislation and procedural mechanisms to deal with the menace of cybercrime. The problem of the difficulties that law enforcement organizations face while attempting to work internationally and such problems as that of cross-border investigation are ignored by it. The paper lacks adequate coverage of the limitations in the control of activities on the Internet as well as the difficulties in surveillance of offenders in cyberspace. There is little reporting of cybercrimes and a complete absence of resources for law enforcement to pursue, investigate, and prosecute these crimes. These areas should have been described in more detail.

One of the books available is **“Policing Cyber Crime” by Petter Gottschalk from 2010,** which can give more understanding in regards to the subject of the study. The investigations related to cybercrimes and the problems that law enforcement organizations face while dealing with cybercrimes are discussed in the book. It also focuses on organisation management and strategy when investigating instances of cybercrime. The book also emphasizes how one has to be in a position to understand the tactics used by would-be perpetrators to lure children online. The main concepts of the book this research work is based upon are shared below: Chapter One: Introduction Chapter Two: Electronic Health Records Chapter Three: Data Protection Strategies Chapter Four: Data Protection Compliance Chapter Five: Data Access Governance Chapter Six: Privacy by Design Chapter Seven: Conclusion Chapter Eight: Appendices The second chapter is dedicated to the presentations of examples of various forms of cybercrime. Again, the fourth chapter contains several criminal notions; still, the role of the police as a party in the fight against cybercrime or their collaboration with other branches of the government is overlooked.

The article entitled “The Legal Policy of Criminal Justice Bureaucracy Cybercrime” by Agus Raharjo,Et Al(2022) gives a review. It identifies the weakness of the legal system of Indonesia for cybercrime as well as the problems encountered in the criminal justice bureaucracy. The authors also posit that the current policies are more or less reactive and are heavily based on what is referred to as the due process model, which does not effectively respond to the dynamic and global phenomenon presented by cybercrime. Both of them have insisted on the call for a paradigm shift and felt that aggression means early detection, prevention as well as the need for rapid response to counter cyber threats. Some of the main points of the article also cover specific problems of police work, such as the absence of appropriate training, lack of sufficient equipment, and the issue of proper jurisdiction in the context of the World Wide Web. Additionally, the authors explain how the collaboration of the government, the private sector, and academic institutions can contribute to the development of a long-term cybersecurity system. They have put forward the need to develop associative structures of public and private sectors for the sharing of information, for the resource exchange in terms of experiences, and for a mutual exchange of knowledge. Yet, there are still some unexplored prospects to discuss, and that is why even this article is affluent in this sense. As with most books of this type, the practical application of proactive models within the Indonesian bureaucracy is given only limited attention, as is a detailed discussion of the training and resource requirements of law enforcement agencies. Also, even though the article focuses on public-private partnerships, it does not include any examples backing up the authors' claims or even case studies.Regarding the forecasts of the consequences of the proposed changes in legislation concerning cybercrime and the effectiveness of the criminal justice system, little is also said. In addition, the article discusses briefly the difficulties of international cooperation in the fight against computer crime. Still, it fails to describe the risks and prospects for the development of measures to strengthen cooperation in this area. Such areas present some concerns for further empirical research, which could help reduce the gaps of knowledge that future research may aim to fill in relation to comprehending cyber criminality within the legal and bureaucratic systems of Indonesia.

Pimploi Tirastittam, Sotarat Thammaboosadee, and Rojjalak Chuckpaiwong article titled "A Study of Bureaucracy in the Digital Transformation Era: A Global Organizational Context," (2018) discusses the issue of the inability of bureaucratic organizations to deal with the issue of digital transformation without addressing the issue of culture. The analyzed study reveals such challenges as lack of flexibility of the hierarchical organization structure and decision making processes, while pointing out the talent management as an opportunity for cultural and digital transition.

Methodology

This research is based on an exploratory , which is qualitative in nature(Scribbr, 2021).This research is designed to follow this approach in order to get a better insight of the problems that the West Bengal police faces in combating cybercrime. This research has used the exploratory research design because cybercrime policing in West Bengal is still a nascent and under-explored field to gain an insight into its dynamics. This is because the current research is somewhat limited and thus an exploratory approach is employed to enable a more detailed examination of the problems that the police encounter, especially in the context of fast growing cybercrime. This method enables the researcher to make changes on the research design as new themes come up thus ensuring that all aspects of the issue have been covered. Moreover, the exploratory research design provides a richness of detail, thus giving an account of the real life situations that police officers encounter while preparing for future research that can expand from the current findings.

The target group of the study includes officers and staff of the West Bengal Cyber Crime Police Station, who are engaged in dealing with cyber crimes in West Bengal. The data were sourced from interviews and Focus Group Discussions. This study was made on the male and female police officers of different ranks who are presently serving in different cybercrime police stations of West Bengal including Murshidabad and Nadia. A semi-structured interview was conducted with the use of open and closed-ended questions to interview the participants in order to capture the main themes that emerged from the interviews. The participants will be chosen in a way that will include both the junior and senior police officers, the new ones in the force, and those who have worked for many years; the target will be 50 participants. In this study, participants were selected purposely, as only police officers who had worked on cybercrime-related cases were chosen.

Research Findings

Data collection at various cybercrime police stations in Murshidabad and Nadia districts of West Bengal has yielded various research findings. The issues encountered during information collection at cybercrime police stations in Murshidabad and Nadia Districts are significant. There are different types of cybercrime. Cybercrime encompasses various forms, such as cyberbullying, cyberstalking, software piracy, social media fraud, and cyberextortion. In these two districts, economic cyber fraud is on the rise. In this case, criminals employ a variety of tactics. Cybercrime is highly organized and has the potential to target anyone. Interviewing numerous cyber victims reveals another aspect: the individuals responsible for cybercrime often lack awareness. Most of the time, victims of cybercrime do not report their experiences to the closest police station. However, the cyber police stations regularly organize various awareness seminars and programs to raise public awareness and combat cybercrime. The fight against cybercrime is tough in West Bengal, India, due to the following challenges: administrative, technological, and resource-based. This thematic analysis discusses the main findings of the study on cybercrime policing in West Bengal, focusing on issues such as police challenges, cybercrime policy formulation, and efforts to increase public awareness and improve policing strategies.

1. Evolving Nature of Cybercrime-

1.A-Post-COVID Shift: The research illustrates a recent shift in the methods used by cybercriminals following the COVID-19 pandemic. This is a result of the growing acceptance and use of innovative technology in the corporate world, particularly in relation to the practice of working from a distance. The existing threats are not inactive; rather, they are escalating and taking advantage of the ongoing global difficulties triggered by the pandemic. The predominant forms of cybercrime reported in the surveyed regions are financial fraud and social media fraud. Hence, the findings are consistent with the general pattern of increasing cybercrime and the widespread existence of criminal syndicates, which requires law enforcement authorities to continuously adjust their strategies. The COVID-19 pandemic has revealed weaknesses in various systems, specifically in the financial sector, which is still susceptible to cyberattacks.

2. Problems that police officers face—

2A- Rapidly Evolving Tactics: Another major drawback is that criminals improve their methods on a regular basis, which puts pressure on the police. These findings prove that it is relatively challenging to arrest new-age offenders with the ability to harness modern technologies and international linkages.

2.B- Resource Constraints: This paper identifies a gap in the available resources, which include technology and personnel who can assist in curbing and combating cybercrime. Poor infrastructure, such as old computers and few cybersecurity personnel, compound this problem.

3.C-Jurisdictional and International Challenges: Cybercrime follows the globalization trend because criminals can work from one country while committing crimes in another country. Cooperation with international organizations is complicated and sometimes sluggish, which compromises the efforts made by the police.

When dealing with cybercrimes, law enforcement must use digital forensics, network monitoring, and malware analysis tools. Nevertheless, the level of technology and training available is limited, which is still a significant disadvantage.

3. Public Awareness and Education—

3A- Awareness campaigns are needed: Thus, the work underlines the importance of increasing the population's awareness of cybersecurity threats and how to prevent them. While leaflet distribution has been part of some activities, the absence of recent awareness camps indicates a lack of emphasis on community participation.

3B- Educational Initiatives: By conducting workshops and incorporating cybersecurity into the curricula, we can take proactive measures to prevent cyber threats in the long run.

General population awareness is an essential factor in the fight against cybercrime. The findings suggest that well-organized and comprehensively conducted awareness-raising campaigns are necessary to equip people and entities for defence against cyber threats. This conforms with international standards, whereby public education is considered one of the most effective ways of combating cybercrimes.

4. Recommendations and Future Goals

4A- Investment in Training and Collaboration: The research suggests that regular training for police officers, engagement of cybersecurity specialists, and public education on cybercrime risks are necessary.

4B-Infrastructure Improvement: There is, therefore, a need to address the challenges of infrastructure in cyber police stations so that there can be an effective method of fighting against these cyber crimes.

Conclusion

As such, the research outcomes provide a detailed description of the cybercrime situation in some regions of West Bengal and the difficulties that the police encounter when fighting cybercrime. The dynamic nature of threats, limited resources, and increased focus on raising general public awareness make the problem less tractable.

To tackle these challenges, more resources must be allocated to the police force, police officers must be regularly trained, and cooperation must be built both at the regional and international levels. Other strategies that should be considered include public enlightenment programs to strengthen society's ability to fight cyber threats. The recommendations given are practical and in tune with international standards and guidelines and provide a way forward towards raising the standards of cyber security in the region.

Reference

1. A DEEP DIVE INTO CYBERCRIME TRENDS IMPACTING INDIA. (n.d.). *Future Crime Research Foundation (FCRF) Whitepaper*.
2. Cybercrime.org.za. (n.d.). *Definition of cybercrime*. Retrieved from https://cybercrime.org.za/definition
3. Vadza, K. C. (2011). Cyber Crime & its Categories. *Indian Journal of Applied Research*, *3*(5), 130–133. https://doi.org/10.15373/2249555x/may2013/39
4. The Indian Express. (2023, September 29). *Victim of cybercrime? Here's a guide on how to file a complaint*. Retrieved from https://indianexpress.com/article/explained/everyday-explainers/victim-cybercrime-guide-how-to-file-complaint-8970419/
5. Harkin, D., Whelan, C., & Chang, L. (2018). The challenges facing specialist police cyber-crime units: an empirical analysis. *Police Practice and Research*, *19*(6), 519–536. https://doi.org/10.1080/15614263.2018.1507889

6. West Bengal Police. (n.d.). *Cyber police stations*. Cyber Crime Wing, Government of West Bengal. Retrieved from https://cybercrimewing.wb.gov.in/PoliceStations
7. National Crime Bureau Report (2022) National Crime Records Bureau. (n.d.). Retrieved form https://ncrb.gov.in/en
8. Factly. (2023, October 31). *Pendency of cybercrime cases has increased in the recent years*. Retrieved from https://factly.in/data-pendency-of-cybercrime-cases-has-increased-in-the-recent-years/
9. News18. (2024). *Kolkata police launches 'Cybuzz' initiative to combat rising cyber crimes*. News18. https://www.news18.com/india/kolkata-police-launches-cybuzz-to-combat-rising-cyber-crimes-8731876.html
10. India Cyber Crime Coordination Centre. (2024). *Cyber digest* (13/02/2024). Retrieved from https://i4c.mha.gov.in/cyber_digest/Feb_2024/I4C%20Daily%20Digest-%2013.02.2024%20.pdf
11. Scribbr. (2021). *Exploratory research*. Scribbr. Retrieved August 26, 2024, from https://www.scribbr.com/methodology/exploratory-research/
12. Tropina, T. (2017). Cyber-policing: the role of the police in fighting cybercrime. *Special Issue 2 Eur. Police Sci. & Res. Bull.*, 287.
13. Gottschalk, P. (2010). *Policing Cyber Crime*. Bookboon.
14. Raharjo, A., Bintoro, R. W., Utami, N. A. T., & Suzuki, M. (2022). The legal policy of criminal justice bureaucracy cybercrime. *Bestuur*, *10*(2), 105-122. https://doi.org/10.20961/bestuur.v10i2.64498
15. Tirastittam, P., Sotarat, T., & Chuckpaiwong, R. (2018). A Study of Bureaucracy in the Digital Transformation Era: A Global Organizational Context. *ITMSOC Transactions on Innovation & Business Engineering*, *3*, 30-34.
16. Reghunadhan, R. (2022). *Cyber Technological Paradigms and Threat Landscape in India*. Palgrave Macmillan.