International Journal of Humanities Social Sciences and Education (IJHSSE)
Volume 11, Issue 7, July 2024, PP 150-161
ISSN 2349-0373 (Print) & ISSN 2349-0381 (Online)
https://doi.org/10.20431/2349-0381.1107014
www.arcjournals.org

Challenges Faced by Police Officers in Investigating Cyber Crime: An Exploratory Study in Bangladesh

Dr. Rukhsana Siddiqua*

Associate Professor, Department of Criminology and Police Science, Mawlana Bhashani Science and Technology University, Santosh, Tangail, Bangladesh

***Corresponding Author**: **Dr. Rukhsana Siddiqua,** Associate Professor, Department of Criminology and Police Science, Mawlana Bhashani Science and Technology University, Santosh, Tangail, Bangladesh*

Abstract: *As time advances, the nature and patterns of crime change. In recent years, there has been an exponential increase in cybercrime victimization, and Bangladesh is no exception. Field-level police officers stationed in police stations regularly receive these complaints and conduct investigations. This study aims to explore the challenges they face regularly while investigating crimes related to cyberspace. Eight Sub inspectors in Tangail and Dhaka participated in in-depth interviews regarding various aspects of cybercrime investigations. This is a qualitative research and exploratory in nature, involving the collection of data from primary sources. Thematic analysis has been implied to analyse data. The study delves into key themes encompassing both internal and external challenges. Internal issues highlighted a lack of logistics support, insufficient training, and the added pressure of other police duties alongside investigations. External hurdles encompass victim non-cooperation, the anonymous nature of criminals, unsatisfactory collaboration with other organizations, and the complex nature of digital evidence, among other factors. The paper concludes by providing recommendations to tackle the challenges faced by the police in investigating cybercrimes.*

Keywords: *Cyber crime, digital evidence, investigation, challenge, tackle.*

1. INTRODUCTION

The concept of cybercrime is continually evolving over time and becoming increasingly sophisticated and diversified (Grabosky, 2014). This poses a formidable challenge in the ongoing battle against it. The definition of "cybercrime" is not universally agreed upon, and there are diverse interpretations and classifications proposed (Alkaabi, Mohay, McCullagh, & Chantler, 2011; Khadam, 2012). At the 10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders, two definitions of cybercrime, specifically narrow and broad, were formulated (United Nations, 2000). In a narrow sense, cybercrime pertains to any illicit actions directed at computer systems or their data. In a broader perspective, it includes any activity wherein computers or networks serve as a tool, target, or location for criminal conduct.

In Bangladesh, the types of cybercrime and the associated punishments are described in the Information and Communication Technology Act, 2006, Digital Security Act of 2018 and the Pornography Control Act, 2012 (Babu,2023) . Cases filed under these laws are tried in Cyber Tribunals, which are established in eight districts: Dhaka, Chattogram, Barishal, Rajshahi, Khulna, Sylhet, Mymensingh, and Rangpur (*Cyber tribunals set up by govt in 8 divisions*, 2021). The Bangladesh Police is the primary government organization responsible for investigating cybercrime cases. They also have specialized units, such as CT-Cyber Crime Investigation under Dhaka Metropolitan Police (DMP) and the Cyber Police Centre in the Criminal Investigation Department (CID), to handle cases that require specialized expertise in the field.

Despite the prevalence of cybercrime, the response of criminal justice to it is inadequate. The cyber tribunal in Dhaka has received 2,669 cases since its formation in 2013 until October 2020

(Asaduzzaman, 2021). Of these, 768 cases have been disposed of, but convictions have only been secured in 22 cases, leading to a cybercrime conviction rate of 2.86%. The victim satisfaction with the services provided by the police after reporting to them is also low. Approximately 80% of the victims feel they did not receive desired help after reporting to the police (Cyber Crime Awareness Foundation, 2023). The low conviction rate and victim dissatisfaction with law enforcement indicate ongoing challenges in investigating cybercrime in Bangladesh. The current study seeks to explore these challenges from the perspective of field-level police officers.

The primary objective of this study is to address the research question, "What challenges do general police officers encounter in the investigation of cybercrime cases?" The following specific objectives have been formulated to achieve this overarching goal:

- To identify the types of cybercrime complaints received by police officers.
- To explore the internal challenges perceived by police officers in the investigation of cybercrime cases.
- To understand the external challenges faced by investigating police officers in the cybercrime cases.

2. METHODOLOGY

This study adopts a qualitative research approach. The nature of this research is exploratory and cross-sectional, involving the collection of data from primary sources. This design is best suited for gaining a comprehensive understanding of the firsthand experience of individuals. Though, there is special branch for cyber crime investigation, but all the police stations have to conduct the primary cyber crime investigation. As the aim of the study is to find out the problems faced by the police, therefore conveniently researcher has recruited respondents from capital city and nearest city of capital of Bangladesh where the occurrences and reporting of cybercrime are noteworthy. Tangail Sadar Model Thana, Tangail Sadar Fari, Mirzapur Thana, and Mohammadpur Thana has been selected randomly.

The target population for this study comprises field-level police officers who have experience in handling cybercrime cases. In Bangladesh, inspectors, sub-inspectors of a police station mainly conduct criminal investigations of such cases. The current study employed snowball sampling for data collection. The study purposively selected and interviewed the first few police officers. Then, the researcher asked them to refer other officers who deals with cyber crimes. This chain-referral method was used to recruit future samples from among their acquaintances. For the study, the data saturation point was 8. This indicates that, after collecting data from 8 respondents further data collection is unlikely to yield additional insights. The primary data in this study were obtained through face-to-face, in-depth interviews with police officers. The interviews were conducted with semi-structured interview guidelines.The researcher conducted these interviews, recorded them, and transcribed the content into a computer. Subsequently, the data were summarized and categorized into codes and themes for analysis. The current research utilized thematic analysis to analyze the collected primary data. Thematic analysis is a prevalent approach in qualitative research, as Braun and Clarke (2006) outline.

In this study, the researcher made diligent efforts to adhere to the ethical guidelines established by the research community. Initially, the researcher transparently disclosed their identity and the purpose of the study to the respondents. Participants were assured that the information they provided would solely be used for academic purposes, and both their data and identity would be kept confidential. Moreover, no monetary incentives were offered to the respondents for their participation in the data collection process. Furthermore, the researcher upheld principles of veracity, carefulness, and other relevant aspects of research ethics throughout the study.

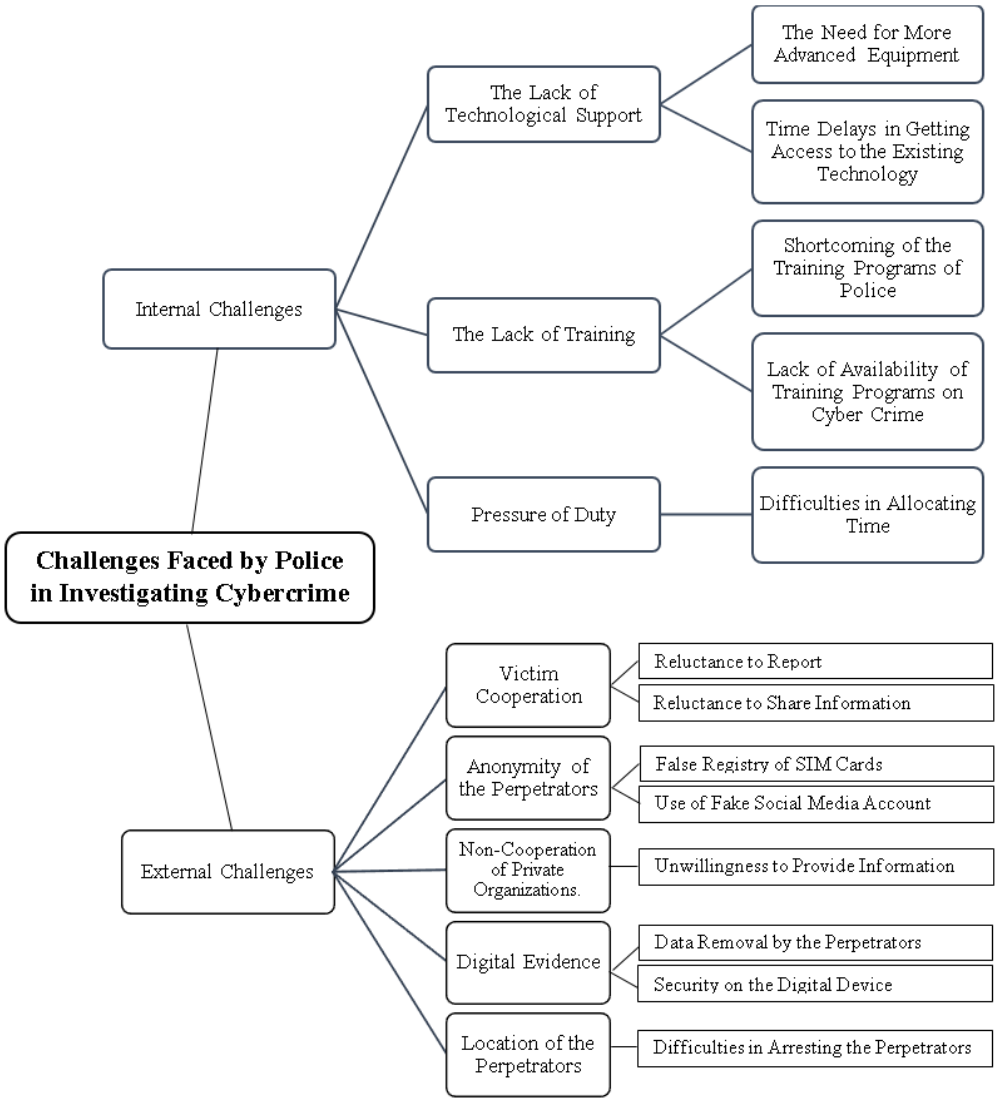

Figure1. *Conceptual framework*

3. FINDINGS

The thematic analysis of the transcripts of the interviews with field-level police officers revealed two distinct themes that describe the challenges faced by them in investigating cybercrime: Internal Challenges and External Challenges. Numerous subthemes also emerged under these themes, which will be discussed in detail in this chapter.

Themes	Subthemes
Internal Challenges	The Lack of Logistic Support
	The Lack of Proper Training
	Pressure of Duty
External Challenges	Victim Non-cooperation
	Anonymity of the Perpetrators
	The Lack of Support from Various Organizations
	Complexity of Digital Evidence
	Diverse Location of the Perpetrators

3.1 Sociodemographic Information

The study primarily reflects the perspectives of police officers with experience in investigating cybercrime. To provide a better understanding of the contextual setting for this qualitative study, socio-demographic information of the respondents has been presented before delving into the thematic analysis.

Table1. *Socio-demographic Characteristics of the Respondents*

Respondent No.	Age (Year)	Gender	Current Workplace	Rank in the Police Force	Experience as Police Officer (Year)	Education
001	31	Male	Tangail Sadar Model Thana	Sub-inspector	3	MSc.
002	36	Male	Mirzapur Thana	Sub-inspector	7	BSc.
003	37	Male	Mirzapur Thana	Sub-inspector	9	BSc.
004	32	Male	Mirzapur Thana	Sub-inspector	3	MBA
005	30	Male	Mohammadpur Thana	Sub-inspector	4	BSc.
006	43	Male	Mohammadpur Thana	Sub-inspector	13	BSc.
007	32	Male	Tangail Sadar Model Thana	Sub-inspector	4	MSc.
008	36	Male	Tangail Sadar Fari	Sub-inspector	8	MS

The table above illustrates that the study's respondents fall within the age range of 30 to 45. All participants are male and currently hold the rank of Sub-Inspectors in the police force. Six of them are stationed in Tangail, while two are based in Dhaka. Additionally, all respondents possess either a graduate or postgraduate degree. Furthermore, each participant in the study has a minimum of three years of experience in the police force.

3.2 The Types of Cybercrime Complaints Received by Police

During in-depth interviews, officers disclosed that the majority of complaints they receive involve cybercrimes, such as social media hacking, the distribution of explicit pictures or videos online, and scams using Bkash.

In incidents of social media hacking, perpetrators gain unauthorized access to victims' Facebook or Emo accounts. Subsequently, they exploit the compromised accounts to deceive friends or relatives into providing money. Some cases also involve ransom demands for the recovery of hacked accounts. The distribution of explicit pictures or videos typically targets women and follows multiple stages. Victims engage in intimate online relationships through social media chats. At a certain point, the victims exchange explicit content or the perpetrator records private video conversations. Blackmail ensues, with the perpetrator seeking money. In many instances, these explicit contents are shared on social media or other websites. Scamming through Bkash involves perpetrators calling individuals and using various social engineering tactics to gain access to their accounts. Typically, they request the OTP code, enabling them to take control of the account and withdraw the funds inside. In addition to the aforementioned prevalent cases, some officers also noted the occurrence of online gambling cases in recent years.

In general, the cases handled by cybercrime police officers predominantly involved individual victims, with a majority of them being women.

3.3 The Internal Challenges

One of the themes that emerged is the challenges that arise within the infrastructure and administration of the police as an organization. These problems are deeply ingrained in the way police are structured and how they function. They encompass a need for more logistics, a deficit in training, and the pressure of routine police duties.

The Lack of Logistic Support

In cases of cybercrime, where the crime itself is committed or enhanced by the use of technology, the use of technology to apprehend the criminal is essential. However, during the interview, most of the officers expressed dissatisfaction with the technological support they receive at their police station when investigating cybercrime. One officer stated:

First of all, the primary challenge is the lack of logistics support. (001)

The police officers participating in this study mainly rely on rudimentary technology like location tracking, call details record analysis, and determining the National Identification of a SIM card. Even these are not readily available at the palm of their hand when they need it. Delays are very common in such cases because of the bureaucratic process of getting access to them. Officers have to undergo troubles in getting technological support from the police headquarters, which they urgently need, and have noted:

Whatever we are currently using, to obtain them, we have to navigate through many processes. They are not readily available to us. We must apply for them first, which comes after so many delays. That's a huge problem. (006)

Suppose, in Tangail district, I have to submit an application to the Police Superintendent for technology, like CDR analysis. But when I urgently need it to identify the perpetrator, immediate technological support is needed. But we don't have that at the station level. (003)

An officer has also expressed his dissatisfaction with the fact that other specialized divisions of the police, such as the Detective Branch or Police Bureau of Investigation, have much better technology at their disposal compared to the general police:

The amount of technological support CID, RAB, or PBI have, we do not get the same level of support. (008)

Several sub-inspectors have exclaimed their desire to have more advanced technology to identify the perpetrators of cybercrime.

In many cases, we desperately need live location tracking of a phone user, a service currently unavailable. I believe only RAB possesses such technology in Bangladesh, but we cannot access it. (001)

Currently, we can only track the tower location; we cannot locate the cell. If we could get the location of the cell, detecting criminals would be so much easier that I cannot express it with words. (007)

Overall, the respondents recognized that there needs to be more technological support, as well as the time delays and other hassles that occur while obtaining them.

The Lack of Proper Training

As a proverb goes, "A man is only as good as his tools." The opposite is also true: A tool is as good as its user. This applies especially in the investigation of cybercrime. The availability of technology and logistic support is only useful if the investigators using it are adequately trained. However, all the participants in this study have expressed some level of discontent with the amount of training they receive regarding the investigation of cybercrime.

In Bangladesh, the sub-inspectors must undergo a year-long training program at Bangladesh Police, located at Sardah. The officers participating in this study have discussed the need for extensive training and focused training on cybercrime. A veteran police officer has exclaimed:

The year-long primary training at Sardah focuses mainly on physical fitness, endurance, and general police duties. I believe cybercrime deserves specific attention, which we did not get. (006)

A young sub-inspector even pointed out the shallowness of the training procedure, stating that it only covers basic theoretical concepts without providing a practical understanding of various issues.

They give us a basic understanding of law and investigation. We also get an overview of various cyber-related crimes and how to deal with them. But, this training only gives us a general idea of what needs to be done. Practical training is essential to carry out these tasks effectively. (004)

After joining the force, police officers have access to various in-service training programs, some of which specifically focus on cybercrime-related issues. However, the effectiveness and duration of these programs have been questioned, as discussed by some participants.

There are some 1 to 5-day sessions. They mainly introduce us to the basic concepts, like theoretical ones. But they are not so helpful or interesting. Most of the time, I fell asleep during the sessions. (001)

Training for 1-2 days won't be sufficient; at least a 15-day or 1-month training is necessary. Because to learn something well, effective learning is necessary. If I go there for just one day, I won't even be able to learn how to turn on a computer. (003)

Even the availability of these in-service training facilities is very limited in quantity. As a result, many do not get access to such programs on time, even though they are very enthusiastic about learning, as pointed out in the interviews. A sub-inspector working at Tangail Model Thana has noted:

... these trainings are so inadequate. And to receive them, a sub-inspector like me has to wait year after year. How will they get training? You tell me. On top of that, a lot of the time it becomes impossible to attend these trainings due to duty pressure. (007)

Another sub-theme that emerged in this study is the inapplicability of traditional tools and investigation techniques to many cybercrimes. Since cybercrime is a recent phenomenon advancing day by day, the conventional approach to investigating crimes may not be well-suited for them. This also indicates the need for regular, up-to-date training programs to address the issue.

In other cases, such as in cases of fighting, there are witnesses, there are people who may have seen the incident, and there are signs of violence. However, in the case of cybercrime, there are no witnesses and no signs of physical violence. It's an entirely different thing. (005)

The prevailing view of the respondents is that there is a substantial need for proper training to enable district-level police officers to conduct effective investigations of cybercrime cases.

The Pressure of Duty

One of the key features of the Bangladesh Police is that they have a myriad of duties to perform, aside from investigations. These include patrolling duties, maintaining law and order in public spaces, preventing public nuisance, executing warrants, and handling political or election duties. It would not be inaccurate to assert that the other duties often take precedence for sub-inspectors, as they occupy most of their time and efforts. The substantial pressure of duty appears to have a negative impact on their investigation of cybercrime cases, as reflected in the interviews with the respondents.

... as thana police, we begin our duties right after waking up, and it continues until around 4 am before we can go to sleep. The constant demands of patrolling, issuing warrants, and other routine tasks leave us with limited time to focus on investigations. (007)

The pressure of duty hampers the investigation of such crime, too. The investigation is a continuous process. You have to give it nonstop effort and intellect to identify the criminal. But because of other duties, we cannot really afford that. (006)

The pressure from the seniors further complicates their situation, as noted by an officer:

You cannot give your best if you are working while seniors are always giving you a hurry. (002)

Since officers juggle multiple tasks while also conducting painstaking investigations of cybercrime, the respondents view it as a major impediment in apprehending criminals and ensuring justice.

3.4 External Challenges

The second theme encompasses the problems faced by the police officers that come from the outside, such as the victim, the perpetrator, various organizations, or the evidence itself. These challenges are mostly inherent to the nature of cybercrime.

Victim's Unwillingness to Cooperate

Victims are one of the core elements of a crime, as well as criminal investigation. Primarily, they are the source of the information upon which an investigation is founded. However, if they are not cooperative with the investigating officer, the task of identifying the perpetrator becomes a very challenging one. Victim non-cooperation is one of the sub-themes that emerged in relation to the external challenges faced by police officers. Participants identified a variety of problems that arise from the side of the victim in investigating cybercrimes. First, some respondents mentioned that the victims or their close relatives often do not report the incident to the police due to embarrassment or concerns about reputation, especially in cases where explicit content of women victims has been distributed online:

... we discovered two more victims besides the student who reported to us. But they did not report it. In many cases, victims feel hesitant to report their cybercrime victimization. [...] In some instances, the victim may come forward. Still, their parents feel hesitated to take the matter to the police due to concerns about their reputation in society. (001)

Secondly, even when the victims report, especially in cases of non-consensual pornography, some officers also faced problems due to the victim not providing enough information or hiding relevant details:

The complainant often hesitates to provide details of the case. We use female police officers to make them feel comfortable and listen to their story in my absence. (007)

They only share what they think is necessary, possibly due to embarrassment or concerns about prestige. However, things do not work like that. A crime does not happen just like that; it takes multiple stages to reach the point of crime. Without knowing all the details about the background, it is challenging for us to conduct a thorough investigation. (006)

In such cases, the distributed explicit contents can be valuable pieces of evidence. But one officer noted that victims often did not want to assist the police officer in finding them, thus creating a hassle for him:

... there are instances where they are reluctant to share certain sensitive content, such as nude pictures. (008)

Non-cooperation from Private Organizations

Half of the respondents faced issues in getting cooperation from third-party organizations in their investigations. These organizations either refuse to assist or take a significant amount of time to respond, causing delays in the investigation process. The problem is particularly noticeable when seeking information from Bkash, a leading mobile finance service in Bangladesh. In cases of Bkash scams, determining the National Identity card linked to the scammer's SIM card is crucial for the investigation. However, Bkash maintains a strict privacy policy regarding user information and refuses to cooperate with police officers, making the investigation of such cases very challenging. A respondent stated:

When we reach out to them directly, they refuse to provide the NID address linked to the registered sim card. Sometimes, they even use their influence. (001)

Another officer expressed his frustration with the hassle he has to go through to get assistance from Bkash:

If you apply today, they tell you to come after 3 days, or maybe after 4 days. There are a lot of hassles. Again, they say, "Go to the office." When you go to that office, they say, "Go to the main office." These matters are a bit troublesome. (005)

In instances where explicit pictures or videos of women are distributed online or used for blackmail, Facebook is mostly used in Bangladesh. Some officers have also felt that Facebook authorities take too much time to provide information about the perpetrator when the police apply to them. For example:

... getting info from there is a bit tricky because you have to apply to Facebook, and they usually don't respond within a month. (004)

Overall, the perceived support received from external organizations was not satisfactory for many respondents.

Anonymity of the Perpetrator

In cases of cybercrime, the perpetrator has the opportunity to maintain anonymity. The majority of the respondents have felt that this greater level of anonymity has caused problems for their investigation. Two major subthemes have emerged related to anonymity. First, the perpetrator uses fake social media accounts to perpetrate his crime, which makes the detection of them very difficult for the officers. An officer has stated:

:*... perpetrators use pseudonyms, and I've encountered such instances. For example, there was a case where a boy, who was Hindu, pretended to be Muslim. He established an affair with a Muslim girl using the pseudonym 'Shimul.' The case involved screen recording of intimate video conversations and blackmailing her with that. I faced some difficulties as the description provided by the girl didn't match with our own findings. (002)*

Another tool used by the criminals to conceal their true identity is the use of a SIM card that has been illicitly registered under someone else's National Identity Card. These types of practices occur in cases of scammers where they deceptively gain access to the Bkash or Nagad account of the victim. A sub-inspector cited:

SIM cards used by a person are sometimes registered under someone else's NID, making it difficult to trace the actual criminal. In such cases, we can identify the NID but struggle to identify the actual person. (001)

Another officer has noted:

There are organized groups that illicitly record multiple registrations of SIM cards under a person's National ID without their knowledge. The unsuspecting individual may not even be aware that a crime is being committed using a SIM card registered under their ID. (002)

In summary, the analysis revealed that the criminal utilizes various tools and techniques to mask his true identity, making the task of the investigator arduous.

Complexity of Digital Evidence

The evidence of cybercrime comes with its own set of challenges. Some officers with experience in seizing electronic device containing evidence, such as phones or laptops, have expressed hurdles during interviews. One of these issues is related to the deletion of vital evidentiary data stored on the device. One of the respondents have noted:

...if the criminal figures out there's an investigation, they can wipe everything clean.(004)

Another issue is the security lock imposed by the perpetrator. A few respondents have faced situations where the perpetrator falsely claims not to know the lock on the device, making it difficult for the investigator to retrieve data from the device:

...sometimes, the phone has security locks or app locks. Perpetrators often do not provide truthful information; they may claim to have forgotten passwords or offer other misleading details. (008)

The respondents also revealed that the forensics team at the Crime Investigation Department has the equipment and necessary knowledge to deal with these challenges, and the general police mainly relies on them in such matters.

Diverse Locations of the Perpetrators

Cybercrimes are, by nature, virtual. The perpetrator can commit the crime from anywhere, whether inside the country or outside. Some of the officers interviewed have pointed that out and expressed their inconvenience in catching the criminal. One officer noted:

The culprit in cybercrime can be located anywhere in the country. I once handled a case filed in Tangail, but the location of the SIM user turned out to be in Jamalpur. This complicates our work.(001)

Another respondent expressed his frustration with the hurdles that emerge due to the transnational nature of cybercrime:

In many cases, the perpetrator has a Facebook account; he is from Bangladesh but is staying abroad. Catching him becomes very difficult. (008)

A few officers also pointed out the bureaucratic hassles, such as informing seniors or seeking cooperation from the police station under whose jurisdiction the criminal is located, that they have to go through when apprehending criminals situated outside the jurisdiction of their police station.

While I can move freely within my thana area at any time, if the case is outside the thana, I need to seek permission from the SP and follow other bureaucratic procedures.(007)

Overall, the issue of jurisdiction concerning crimes within the country was perceived more as an inconvenience than a major concern among the respondents.

4. Conclusion

The study found that district-level police officers face numerous challenges when dealing with cybercrime. The research looks into these issues from the officers' perspective, revealing problems like limited technological support, deficiencies in available training, a lack of more specialized training, and considerable pressure from non-investigation duties. The study also explored other challenges specific to cybercrime cases, including victim non-cooperation, the reluctance of private organizations to support investigations, the intricate and volatile nature of digital evidence, jurisdictional complexities linked to the perpetrator's location, and the heightened level of anonymity. These challenges are perceived to significantly affect the outcomes of investigations and the prosecution of offenders. Therefore, the study aims to suggest ways to improve the investigation process and overall law enforcement response to cybercrime.

5. Recommendations

Based on the study findings, the researcher presents the following recommendations. The results indicate that the current state of the general police in Bangladesh concerning cybercrime investigation is suboptimal due to various challenges. The recommendations primarily aim to enhance the overall efficiency of the general police in Bangladesh in investigating cybercrime. These recommendations are derived from both the insights of the respondents and the researcher's perspective.

1. Equip each police station with modern equipment and devices essential for investigating cybercrime and detecting perpetrators.

2. Integrate an adequate number of modules on cybercrime and digital forensics into the one-year-long primary training for newly recruited sub-inspectors at the Bangladesh Police Academy, Sardha, Rajshahi.

3. Ensure regular in-service training programs for officers to keep them updated with the latest innovations in the field of cybercrime investigations.

4. Ensure police stations are adequately staffed to alleviate the pressure of routine police duties on officers.

5. Establish proper collaboration between the police and private organizations in the battle against cybercrime.

6. Raise widespread awareness among the general public regarding cybercrime and its prevention. 7. Implement strict government-level policies to prevent the fraudulent registration of multiple SIM cards under National ID cards.

REFERENCES

ActionAid Bangladesh. (2022). Online Violence Against Women in Bangladesh. Retrieved from https://www.actionaidbd.org/storage/app/media/Research%20Findings_Online%20Violence%20Against%20Women.pdf

Ali, B. G. S. M. R. (2018). Digital Evidence–An Approach to Safeguard from Cybercrime in Bangladesh. *NDC E-JOURNAL, 17*(1), 23-41.

Alkaabi, A., Mohay, G. M., McCullagh, A., & Chantler, N. (2011). Dealing with the Problem of Cybercrime. In *Springer eBooks* (pp. 1–18). https://doi.org/10.1007/978-3-642-19513-6_1

Asaduzzaman. (2021, September 20). *Cybercrime: 97 per cent cases dismissed*. Prothomalo. https://en.prothomalo.com/bangladesh/crime-and-law/cyber-crime-97-per-cent-cases-dismissed

Babu, K. E. K. (2023, January). The Reality of Cyber Security in Bangladesh, Relevant Laws, Drawbacks and Challenges. In *Cybersecurity in the Age of Smart Societies: Proceedings of the 14th International Conference on Global Security, Safety and Sustainability, London, September 2022* (pp. 89-104). Cham: Springer International Publishing.

Bari, H. M. F. (2015). An Appraisal of Criminal Investigation in Bangladesh: Procedure and Practice. *Journal of the Asiatic Society of Bangladesh (Humanities)[2015]*, *60*(2), 139-159.

Barkat, A., & Kashem, M. B. (2020) *Title of the Report: A Study On Forensic Services in Criminal Investigation in Bangladesh*. Human Development Research Centre (HDRC). Retrieved from https://www.hdrc-bd.com/a-study-on-forensic-services-in-criminal-investigation-in-bangladeshimpacts-challenges-and-capacity-building-issues-conducted-for-bangladesh-police-cid-dhaka-year-2020/

Biasiotti, M. A., Cannataci, J. A., Bonnici, J. P. M., & Turchi, F. (2018). Introduction: Opportunities and Challenges for Electronic evidence. In *Law, governance and technology series* (pp. 3–12). https://doi.org/10.1007/978-3-319-74872-6_1

Bossler, A., & Holt, T. (2016). On the need for policing cybercrime research. *ACJS Today*, *41*(1), 14.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Brenner, S. W. (2006). Cybercrime jurisdiction. *Crime, law and social change*, *46*, 189-206.

Brenner, S. W. (2007). Private-public sector cooperation in combating cybercrime: In search of a model. *J. Int'l Com. L. & Tech.*, *2*, 58.

Chaiken, J. M., Greenwood, P. W., & Petersilia, J. (1977). The criminal investigation process: A summary report. *Policy Analysis*, 187-217.

Creswell, J. W., & Creswell, J. D. (2018). Research design: qualitative, quantitative, and mixed methods approaches.

Cyber Crime Awareness Foundation. (2023, May 20). Cyber Crime Trend in Bangladesh-2023. Retrieved from https://ccabd.org/wp-content/uploads/2023/09/CCAF_ResearchReport_2023_May_20-V8.pdf

Cyber tribunals set up by govt in 8 divisions. (2021, April 6). The Daily Star. https://www.thedailystar.net/law-our-rights/law-news/news/cyber-tribunals-set-govt-8-divisions-2073209

Dawson, M. (2020). Cybercrime: Internet Driven Illicit Activities and Behavior. *Land Forces Academy Review*, *25*(4), 356-362.

De Paoli, S., Johnstone, J., Coull, N., Ferguson, I., Sinclair, G., Tomkins, P., Brown, M. C., & Martin, R. (2020b). A Qualitative Exploratory Study of the Knowledge, Forensic, and Legal Challenges from the Perspective of Police Cybercrime Specialists. *Policing: A Journal of Policy and Practice*, *15*(2), 1429–1445. https://doi.org/10.1093/police/paaa027

El-Guindy, M. N. (2008). Cybercrime in the Middle East. Retrieved from http://www.cybercrimejournal.co.nr

Faruque, A. A. (2007). Goals and purposes of criminal justice system in Bangladesh: An evaluation. *Bangladesh Journal of Law, 10.* Retrieved from https://www.biliabd.org/wp-content/uploads/2021/08/Dr.-Abdullah-Al-Farooque.pdf

Grabosky, P. (2014c). The Evolution of Cybercrime, 2004-2014. *Social Science Research Network*. https://doi.org/10.2139/ssrn.2535605

Hadlington, L., Lumsden, K., Black, A., & Ferra, F. (2018b). A qualitative exploration of police officers' experiences, challenges, and perceptions of cybercrime. *Policing: A Journal of Policy and Practice*, *15*(1), 34–43. https://doi.org/10.1093/police/pay090

Harkin, D., Whelan, C., & Chang, L. Y. (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

Holland, B. J. (2020b). Transnational cybercrime. In *IGI Global eBooks* (pp. 108–128). https://doi.org/10.4018/978-1-5225-9715-5.ch007

Jeffries, S., & Apeh, E. (2020). Standard operating procedures for cybercrime investigations: a systematic literature review. *Emerging Cyber Threats and Cognitive Vulnerabilities*, 145-162.

Kader, S., & Minnaar, A. (2015). Cybercrime investigations: Cyber-processes for detecting of cybercriminal activities, cyber-intelligence and evidence gathering. *Acta Criminologica: African Journal of Criminology & Victimology*, *2015*(sed-5), 67-81.

Kashem, M. B. (2017). Issues and challenges of police investigative practices in Bangladesh: An empirical study. *Crime, Criminal Justice, and the Evolving Science of Criminology in South Asia: India, Pakistan, and Bangladesh*, 273-295.

Khadam, N. (2012). Insight to Cybercrime. *법학논총*, *29*(1), 55-80.

Kleijssen, J., & Perri, P. (2017). Cybercrime, evidence and territoriality: Issues and options. In *Netherlands Yearbook of International Law 2016: The Changing Nature of Territoriality in International Law* (pp. 147-173). The Hague: TMC Asser Press.

Kramer, X. E. (2018, September). Challenges of electronic taking of evidence: old problems in a new guise and new problems in disguise. In *Il Conferencia Internacional & XXVI Jornadas Iberoamericanas de Derecho Procesal IIDP & IAPL, La Prueba en el Proceso/Evidence in the process Atelier* (pp. 391-410).

Labu, N. (2018, May 19). Most fraudulent SIMs being used by criminals. *Dhaka Tribune*. https://www.dhakatribune.com/bangladesh/crime/145978/most-fraudulent-sims-being-used-by-criminals

Leppänen, A., & Kankaanranta, T. (2017). Cybercrime investigation in Finland. Journal of Scandinavian Studies in Criminology and Crime Prevention, 18(2), 157–175. https://doi.org/10.1080/14043858.2017.1385231

Leppänen, A., & Kankaanranta, T. (2017b). Cybercrime investigation in Finland. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, *18*(2), 157–175. https://doi.org/10.1080/14043858.2017.1385231

Maras, M.-H. (2016). *Cybercriminology*. Oxford University Press.

McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. *Summary of key findings and implications. Home Office Research report*, *75*, 1-35.

Mia, B. (2021). Cybercrime and Its Impact in Bangladesh: a quest for necessary legislation. *International Journal of Law and Legal Jurisprudence Studies, 2*(4).

Roussev, V. (2016b). Digital Forensic Science: issues, methods, and challenges. *Synthesis Lectures on Information Security, Privacy, and Trust*, *8*(5), 1–155. https://doi.org/10.2200/s00738ed1v01y201610spt019

Saariluoma, P., & Sacha, H. (2014). How cyber breeds crime and criminals. *The society of digital information and wireless communications (SDIWC)*.

Sabillon, R., Cavaller, V., Cano, J., & Serra-Ruiz, J. (2016, June). Cybercriminals, cyberattacks and cybercrime. In *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)* (pp. 1-9). IEEE.

Sachowski, J. (2016b). Understanding digital forensics. In *Elsevier eBooks* (pp. 3–16). https://doi.org/10.1016/b978-0-12-804454-4.00001-0

Sarre, R., Lau, L. Y. C., & Chang, L. Y. (2018). Responding to cybercrime: current trends. *Police practice and research*, *19*(6), 515-518.

Senjo, S. R. (2004). An analysis of computer-related crime: Comparing police officer perceptions with empirical data. *Security Journal*, *17*, 55-71.

Sindhu, K. K., & Meshram, B. B. (2012b). Digital forensics and Cyber Crime datamining. *Journal of Information Security*, *03*(03), 196–201. https://doi.org/10.4236/jis.2012.33024

Smith, R. G. (2005). Impediments to the successful investigation of transnational high tech crime.

Startling rise in cybercrime cases. (2023, January 17). Bangladesh Post. https://bangladeshpost.net/posts/startling-rise-in-cybercrime-cases-103824

United Nations. (2000). Crimes Related to Computer Networks: Background Paper for the Workshop on Crimes Related to the Computer Network. Retrieved from https://www.unodc.org/documents/congress/Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks.pdf

Watt, A. C., & Slay, J. (2015). First responders actions to cope with volatile digital evidence. *International Journal of Electronic Security and Digital Forensics*, *7*(4), 381-399.

Yesmen, N., & Ahmed, N. (2022). The Nature and Challenges of Cyber Policing: A Study on Criminal Investigation Department (CID), Dhaka, Bangladesh. *Asian Journal of Sociological Research*, *5*(1), 210–214. Retrieved from https://globalpresshub.com/index.php/AJSR/article/view/1667

AUTHORS' BIOGRAPHY

Dr. Rukhsana Siddiqua was born in Bangladesh in the year 1987. She completed her graduation (B.Sc. Honors) and post-graduation (MS) in criminology and police science. She was involved in several national level surveys from student life. She joined as Research Assistant in Bangladesh Women Lawyers' Association in 2010. Then she joined as Lecturer at the department of Criminology and Police Science of Mawlana Bhashani Science and Technology University, Bangladesh in 2012 and promoted as Assistant Professor in the year 2014 and as Associate Professor in 2019. Meanwhile, she accomplished post graduation in Victimology and Victim Assistance, offered by World Society of Victimology, at City University of Hong Kong, Hong Kong in 2018 and completed her PhD in cyber violence victimization from the Jindal Institute of Behavioral Sciences of O.P. Jindal Global University, Haryana, India in 2024. She developed her expertise in different fields of criminology and victimology. She is a life member of World Society of Victimology; Country Director of South Asian Society of Criminology and Victimology and member of Bangladesh Society of Criminology and Victimology. The author's major fields of study are cybercrime, juvenile delinquency, trafficking, security and criminal investigation.

Citation: *Dr. Rukhsana Siddiqua., "Challenges Faced by Police Officers in Investigating Cyber Crime: An Exploratory Study in Bangladesh" International Journal of Humanities Social Sciences and Education (IJHSSE), vol 11, no. 7, 2024, pp. 150-160. DOI: https://doi.org/10.20431/2349- 0381.1107014.*