Factors Affecting the Awareness of Cybercrimes, Cybercrime Investigation, and Digital Forensics among Law Enforcement Agencies

Nisheeth Dixit

Bharti School of Telecommunication Technology and Management

Indian Institute of Technology Delhi

APRIL 2025

Factors Affecting the Awareness of Cybercrimes, Cybercrime Investigation, and Digital Forensics among Law Enforcement Agencies

by

Nisheeth Dixit

Bharti School of Telecommunication Technology and Management

Submitted

in fulfilment of the requirements of the degree of
Doctor of Philosophy

to the

Indian Institute of Technology Delhi
April 2025

Certificate of the Supervisors

This is to certify that the thesis titled '**Factors Affecting the Awareness of Cybercrimes, Cybercrime Investigation and Digital Forensics Among Law Enforcement Agencies**,' which is being submitted by Mr. Nisheeth Dixit to the Bharti School of Telecommunication Technology and Management, Indian Institute of Technology Delhi, for the award of the degree of Doctor of Philosophy (PhD) is a record of bonafide research work carried out by him. He has worked under my supervision in conformity with the rules and regulations of the Indian Institute of Technology, Delhi. The research reports, and results presented in the thesis have not been submitted in part or full for the award of any degree or diploma in any other university or institute.

Date: 22 January 2024

New Delhi

Prof Mahim Sagar

Professor

Department of Management Studies

Indian Institute of Technology, Delhi

New Delhi, India

Dr Gaurav Gupta

Additional Director

Ministry of Electronics and Information Technology, Government of India

New Delhi, India

Dedicated to

This Ph.D. "Thesis" is dedicated to my respected parents Dr. Rajendra Kumar Dixit, Smt. Vijaya Dixit and my respected in-laws Sh. Satya Prakash Sharma, Smt. Usha Sharma. My indebtedness to them cannot be expressed in words.

Acknowledgments

The research on '**Factors Affecting the Awareness of Cybercrimes, Cybercrime Investigation and Digital Forensics Among Law Enforcement Agencies** was a long journey. During this journey of long working hours, in-depth discussions, intensive analysis, and academic pursuit, I was fortunate to get the support, guidance, and encouragement from many whom I am indebted to.

First and foremost, I express my heartfelt gratitude to my research guides, Professor Mahim Sagar, Department of Management Studies, IIT Delhi, and Dr Gaurav Gupta, Additional Director, Ministry of Electronics and Information Technology, Government of India, New Delhi.

Prof. Mahim Sagar has profound knowledge and experience in marketing, brand management, marketing not-for-profit, ethical branding, and policy research. He is associated with several prestigious projects with the government of India and Non-Government Organizations. Prof. Sagar provided invaluable insights about 'Grounded Theory Methodology (GTM)' and took me through the process of understanding and applying them to my research. His constant mentoring during my research helped me go through the process with academic rigor. His long sessions of intense discussions were vital to keep me focused and grounded.

Dr Gaurav Gupta brought with him immense knowledge and practical experience in digital forensics. In the Ministry of Electronics and Information Technology, he dealt with court cases related to the IT Act, the scheme of 79A labs, and R&D projects related to cyber security. His profound knowledge and understanding of digital forensics gave my research the necessary depth and punch.

I am grateful to Prof. Ravi Shankar, professor at the Department of Management Studies, IIT Delhi, and Chairperson of my 'Student Research Committee.' His strong support and encouragement motivated me to work hard. During the course of my research, his continuous monitoring of progress, along with research-oriented guidance, helped me remain goal-oriented. His academic insights and scholarly advice provided an edge to my research.

I sincerely thank members of my 'Student Research Committee,' Prof. V.K. Panigrahi, IIT Delhi, and Dr. Somitra Sanadhya, IIT Jodhpur, for their incredible support and input during the research. Their clarity and focused and strategic approach to the subject immensely contributed to my research.

I acknowledge the support of Ms. Charru Hasti, project consultant and research scholar under the supervision of Prof. Mahim Sagar at IIT Delhi. Her understanding of MAXQDA visualization techniques provided excellent support to my research.

I thank Ms. Shefali Khare, Ms. Delma Momi, and Ms. Shyamalambica Peri for their sincere assistance and support.

I am indebted to my participants, who devoted long hours to discussions and interviews despite their busy schedules and sensitivity to the subject and their jobs. These interviews were the bedrock of my research as a primary data source. Some have handled and supervised important and sensitive cybercrime cases and have exceptional and practical knowledge of cybercrime investigation and digital forensic examination.

I sincerely thank my elder brother, Mr. Ruchin Dixit, and family, Smt. Shalini Dixit, Mudit Dixit and Dhwani Dixit for their support.

I would not be able to complete my acknowledgment without mentioning my family's unprecedented, exceptional, strong, untiring, and dedicated support. My wife, Prof. (Dr) Aparna Dixit, and my daughter, Ms. Tavishee Dixit, were my source of inspiration, strength, and energy. During this long journey, I took away some precious moments from them. The time I should have spent with them was spent on my research. I always got their support and encouragement. I express my deepest love and appreciation for their support.

Nisheeth Dixit

(2016BSZ8042)

Abstract

The research on '**Factors Affecting the Awareness of Cybercrimes, Cybercrime Investigation and Digital Forensics Among Law Enforcement Agencies**' was based on exploratory qualitative research design. The study used 'Grounded Theory Methodology' (GTM) by Corbin and Strauss.

Cybercriminals leverage emerging technologies to advance their malicious motives and commit new-age cybercrimes. The victims of cybercrimes are unaware of the changing modus *operandi* of cybercriminals. They are also unaware of how to report cybercrimes and what remedies are available. There is a small conversion rate of cybercrime complaints into First Information Reports (FIR). Law Enforcement Agencies are facing challenges in the investigation and prosecution of new age cybercrimes, States Police coordination, logistics problems, investigation abroad, lack of standard operating procedure for collection and preservation of electronic evidence, admissibility of electronic evidence, challenges with Forensic labs.

Limited literature is available on awareness of cybercrime, cybercrime investigation challenges, and digital forensic challenges among law enforcement agencies. Therefore, a qualitative research method for exploration has been used. This research aims to explore the factors that affect the Awareness of Cybercrimes, Cybercrime Investigation, and Digital Forensics among Law Enforcement Agencies. This research problem addresses several questions in the three sub-areas: Cybercrimes, Cybercrime Investigation, and Digital Forensics. These are- Cybercrimes: (1) what are the top cybercrimes in India, and what are the motives of cybercrimes? (2) What is the level of awareness of cybercrimes and cyber laws among law enforcement agencies? (3) What are the challenges in less reporting of cybercrimes? (4) Why is there a low conversion rate of complaints into FIR? (5) How can financial loss in cybercrime cases be prevented? Cybercrime Investigation: (1) What challenges do law enforcement agencies face regarding the legal, operational, technical, investigation procedural, and organizational challenges? (2) What are the prosecution challenges during the trial of cybercrime cases? (3) What majors have been taken for

cybercrime victim awareness, compensation, and attachment of property of cybercrime accused persons? Digital Forensics: (1) What are the significant digital forensic challenges? (2) What are the technical issues in forensic examination? (3) What are the challenges with Anti forensics? (4) What challenges are faced by Investigating officers and forensic experts? (5) What challenges do Forensic Labs face? (6) Why is there a pendency before forensic labs? (7) What are privacy and digital forensics challenges?

These questions have been answered by achieving the following three research objectives.

RO1. Explore the legal and technological challenges in cybercrime investigation and digital forensics.

RO2. Validate the challenges discovered using case studies.

RO3. Suggest a legal framework for mitigation of the challenges in the investigation of crimes in cyberspace.

Regarding the inclusion of the hypothesis/propositions, I wish to submit that this research is exploratory in nature, and validation is done through case studies. We have deployed an inductive approach since we are not testing or contextualizing an existing theory in the above studies. Here, the hypothesis and proposition are not predefined.

The primary data collection method was in-depth interviews, which enabled the collection of rich data from participants based on their personal experiences while maintaining focus on the research questions. MAXQDA 2020 software was used for 'Computer Assisted Qualitative Data Analysis Software (CAQDAS).

The research was carried out after identifying the research gap in the literature review, indicating that 'Cybercrimes,' 'Cybercrime investigation,' and 'Digital Forensics' were emerging concepts. No research could be found that had focused on this subject from an Indian Perspective.

The context for the research was chosen as Cybercrimes, Cybercrime investigation, and Digital Forensics, and it was carried out from an Indian perspective. The research covered the period from 2001 to 2023. The Indian perspective was critical due to emerging

cybercrimes and challenges faced by law enforcement agencies in the country. The research was based on the analysis of in-depth interviews of Indian law enforcement officers and forensic experts on cybercrime investigation and digital forensic analysis of electronic evidence, who have wide-ranging experience, including practical exposure in handling and supervising cybercrime cases.

The study identifies the challenges law enforcement officers, forensic experts and forensic labs are facing in handling cybercrime cases and digital forensic analysis.

Additionally, for policymakers, the research suggests the implementation of cybercrime awareness and prevention strategies, effective cybercrime reporting and response mechanism, victim compensation framework, regular training and skill enhancement of Law Enforcement officers, Forensic experts, Prosecution and Judicial officers, establishment of a National Cyber Investigative Joint Task Force, Special Fast track courts (SFTCs) for cybercrime matters at district level, Examiner of Electronic Evidence(EEE) Labs in every state**.** The research further suggests that new cyber offenses should be covered in the upcoming Digital India Act, and paramount attention should be given to legal, technical, operational, procedural, organizational, resource, and other challenges highlighted in the research study.

सार

'कानून प्रवर्तन एजेंसियों के बीच साइबर अपराध, साइबर अपराध जांच और डिजिटल फोरेंसिक के बारे में जागरूकता को प्रभावित करने वाले कारक' पर शोध खोजपूर्ण गुणात्मक अनुसंधान डिजाइन पर आधारित था। अध्ययन में कॉर्बिन और स्ट्रॉस की 'ग्राउंडेड थ्योरी मेथडोलॉजी' (जीटीएम) का इस्तेमाल किया गया।

साइबर अपराधी अपने दुर्भावनापूर्ण उद्देश्यों को आगे बढ़ाने और नए जमाने के साइबर अपराध करने के लिए उभरती प्रौद्योगिकियों का लाभ उठाते हैं। साइबर अपराध के शिकार लोगों को साइबर अपराधियों के बदलते तौर-तरीकों के बारे में जानकारी नहीं होती है। वे इस बात से भी अनभिज्ञ हैं कि साइबर अपराधों की रिपोर्ट कैसे करें और क्या उपाय उपलब्ध हैं। साइबर अपराध की शिकायतों को प्रथम सूचना रिपोर्ट (एफआईआर) में बदलने की दर बहुत कम है। कानून प्रवर्तन एजेंसियों को नए युग के साइबर अपराधों की जांच और अभियोजन, राज्य पुलिस समन्वय, परिवहन से संबंधित समस्याओं, विदेश में जांच, इलेक्ट्रॉनिक साक्ष्य के संग्रह और संरक्षण के लिए मानक संचालन प्रक्रिया की कमी, इलेक्ट्रॉनिक साक्ष्य की स्वीकार्यता, फोरेंसिक लैब को चुनौतियों का सामना करना पड़ रहा है

साइबर अपराधों और उनकी जांच पर उपलब्ध साहित्य सीमित है और कानून प्रवर्तन एजेंसियों के बीच साइबर अपराध, साइबर अपराध जांच चुनौतियों और डिजिटल फोरेंसिक चुनौतियों के बारे में जागरूकता का उल्लेख नहीं करता है। अतः अन्वेषण के लिए गुणात्मक शोध पद्धति का प्रयोग किया गया है। इसलिए, इस शोध का उद्देश्य उन कारकों का पता लगाना है जो कानून प्रवर्तन एजेंसियों के बीच साइबर अपराध, साइबर अपराध जांच और डिजिटल फोरेंसिक के बारे में जागरूकता को प्रभावित करते हैं। यह शोध समस्या तीन उप-क्षेत्रों में कई प्रश्नों का समाधान करती है: साइबर अपराध, साइबर अपराध जांच और डिजिटल फोरेंसिक। ये हैं- साइबर अपराध: (1) भारत में शीर्ष साइबर अपराध कौन से हैं, और साइबर अपराध के उद्देश्य क्या हैं? (2) कानून प्रवर्तन एजेंसियों के बीच साइबर अपराधों और साइबर कानूनों के बारे में जागरूकता का स्तर क्या है? (3) साइबर अपराधों की कम रिपोर्टिंग में क्या चुनौतियाँ हैं? (4) शिकायतों को एफआईआर में बदलने की दर कम क्यों है? (5) साइबर क्राइम के मामलों में वित्तीय नुकसान को कैसे रोका जा सकता है? साइबर अपराध जांच: (1) कानूनी, परिचालन, तकनीकी, जांच प्रक्रियात्मक और संगठनात्मक चुनौतियों के संबंध में कानून प्रवर्तन एजेंसियों को किन चुनौतियों का सामना करना पड़ता है? (2) साइबर अपराध मामलों की सुनवाई के दौरान अभियोजन की चुनौतियाँ क्या हैं? (3) साइबर अपराध पीड़ित जागरूकता, मुआवजा और साइबर अपराध के आरोपी व्यक्तियों की संपत्ति की कुर्की के लिए क्या कदम उठाए गए हैं?

डिजिटल फोरेंसिक: (1) महत्वपूर्ण डिजिटल फोरेंसिक चुनौतियाँ क्या हैं? (2) फोरेंसिक जांच में तकनीकी मुद्दे क्या हैं? (3) एंटी फोरेंसिक के साथ क्या चुनौतियाँ हैं? (4) जांच अधिकारियों और फोरेंसिक विशेषज्ञों को किन चुनौतियों का सामना करना पड़ता है? (5)फॉरेंसिक लैब्स को किन चुनौतियों का सामना करना पड़ता है? (6)फॉरेंसिक प्रयोगशालाओं के समक्ष लंबित मामले क्यों हैं?(7)गोपनीयता और डिजिटल फोरेंसिक चुनौतियां क्या हैं?

निम्नलिखित तीन शोध उद्देश्यों को प्राप्त करके इन प्रश्नों का उत्तर दिया गया है।

आरओ1. साइबर अपराध जांच और डिजिटल फोरेंसिक में कानूनी और तकनीकी चुनौतियों का अध्ययन और खोज करें।

आरओ2. केस स्टडीज का उपयोग करके खोजी गई चुनौतियों का सत्यापन करें।

आरओ3. साइबरस्पेस में अपराधों की जांच में चुनौतियों को कम करने के लिए एक कानूनी ढांचा सुझाएं

प्राथमिक डेटा संग्रह विधि गहन साक्षात्कार थी, जो शोध प्रश्नों पर ध्यान केंद्रित रखते हुए प्रतिभागियों से उनके व्यक्तिगत अनुभवों के आधार पर समृद्ध डेटा एकत्र करने में सक्षम थी। MAXQDA 2020 सॉफ्टवेयर का उपयोग 'कंप्यूटर असिस्टेड क्वालिटेटिव डेटा एनालिसिस सॉफ्टवेयर (CAQDAS)' के लिए किया गया था।

यह शोध साहित्य समीक्षा में शोध अंतर की पहचान करने के बाद किया गया था, जो दर्शाता है कि 'साइबर अपराध,' 'साइबर अपराध जांच,' और 'डिजिटल फोरेंसिक' उभरती हुई अवधारणाएं थीं। ऐसा कोई शोध नहीं मिल सका जो भारतीय परिप्रेक्ष्य से इस विषय पर केंद्रित हो।

शोध के लिए संदर्भ को साइबर अपराध, साइबर अपराध जांच और डिजिटल फोरेंसिक के रूप में चुना गया था, और इसे भारतीय परिप्रेक्ष्य से किया गया था। शोध में 2001 से 2023 तक की अवधि को शामिल किया गया। देश में उभरते साइबर अपराधों और कानून प्रवर्तन एजेंसियों के सामने आने वाली चुनौतियों के कारण भारतीय परिप्रेक्ष्य महत्वपूर्ण था। यह शोध साइबर अपराध जांच और इलेक्ट्रॉनिक साक्ष्य के डिजिटल फोरेंसिक विश्लेषण पर भारतीय कानून प्रवर्तन अधिकारियों और फोरेंसिक विशेषज्ञों के गहन साक्षात्कार के विश्लेषण पर आधारित था, जिनके पास साइबर अपराध मामलों को संभालने और पर्यवेक्षण करने में व्यावहारिक अनुभव सहित व्यापक अनुभव है।

अध्ययन साइबर अपराध मामलों और डिजिटल फोरेंसिक विश्लेषण से निपटने में कानून प्रवर्तन अधिकारियों और फोरेंसिक विशेषज्ञों के सामने आने वाली चुनौतियों की पहचान करता है।

इसके अतिरिक्त, नीति निर्माताओं के लिए, शोध साइबर अपराध जागरूकता और रोकथाम रणनीतियों, प्रभावी साइबर अपराध रिपोर्टिंग और प्रतिक्रिया तंत्र, पीड़ित मुआवजा ढांचे, कानून प्रवर्तन अधिकारियों, फोरेंसिक विशेषज्ञों, अभियोजन और न्यायिक अधिकारियों के नियमित प्रशिक्षण और कौशल वृद्धि, एक राष्ट्रीय साइबर जांच संयुक्त कार्य बल की स्थापना, जिला स्तर पर साइबर अपराध मामलों के लिए विशेष फास्ट ट्रैक अदालतें (एसएफटीसी), हर राज्य में इलेक्ट्रॉनिक साक्ष्य के परीक्षक (EEE) प्रयोगशालाओं की स्थापना की जानी चाहिए। शोध आगे सुझाव देता है कि नए साइबर अपराधों को आगामी डिजिटल इंडिया अधिनियम में शामिल किया जाना चाहिए और शोध अध्ययन में उजागर की गई कानूनी, तकनीकी, परिचालन, प्रक्रियात्मक, संगठनात्मक, संसाधन और अन्य चुनौतियों पर सर्वोपरि ध्यान दिया जाना चाहिए।

Table of Contents

List of the Tables

List of the Figures