

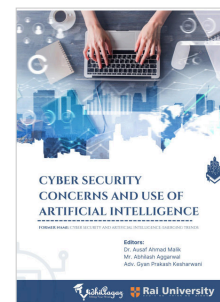
CHAPTER 17

Role of Police in Investigating Digital Crimes

Siddharth Baskar

in *Cyber Security Concerns and Use of Artificial Intelligence*, edited by Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani (VidhiAagaz 2024), pp. 145–149

ISBN 978-81-947620-5-8



CITATIONS

BLUEBOOK (21ST ED.)

Siddharth Baskar, *Role of Police in Investigating Digital Crimes*, in CYBER SECURITY CONCERNS AND USE OF ARTIFICIAL INTELLIGENCE 145 (Ausaf Ahmad Malik, Abhilash Aggarwal & Gyan Prakash Kesharwani eds., VidhiAagaz 2024).

OSCOLA (4TH ED.)

Siddharth Baskar, ‘Role of Police in Investigating Digital Crimes’ in Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani (eds), *Cyber Security Concerns and Use of Artificial Intelligence* (VidhiAagaz 2024) 145.

CHICAGO (17TH ED.)

Baskar, Siddharth. “Role of Police in Investigating Digital Crimes.” In *Cyber Security Concerns and Use of Artificial Intelligence*, edited by Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani, 145–149. Maihar: VidhiAagaz, 2024. <https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-17/>.

APA (7TH ED.)

Baskar, S. (2024). Role of police in investigating digital crimes. In A. A. Malik & A. Aggarwal & G. P. Kesharwani (Eds.), *Cyber security concerns and use of artificial intelligence* (pp. 145–149). VidhiAagaz. <https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-17/>

SOURCE

<https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-17/>

RIGHTS

Free to read online. © VidhiAagaz 2024. All rights reserved: no part of this publication may be copied, reproduced, adapted or transmitted in any form or by any means without the prior written permission of the publisher.

Citations are given as a guide; check them against the style manual you follow. This page was added by VidhiAagaz to the downloaded file. The chapter follows, with the page numbers of the printed book.

ROLE OF POLICE IN INVESTIGATING DIGITAL CRIMES

Siddharth Baskar²²

ABSTRACT

The development of technology and the improvement of connectivity have made it easier to share information and provide services; however, they also present a significant challenge because of the increased vulnerability to the escalation of digital crimes on a global scale. Increasing public awareness and protecting citizens from the dangers of digital crimes are two of the most important roles that the police play. As a crucial framework for protecting individuals and imposing substantial penalties on wrongdoers for their misconduct, the Information Technology Act of 2000 ("IT Act") serves as a crucial framework. The law enforcement agencies need to work together with cybersecurity experts from both the national and international levels to enhance their capabilities in dealing with the negative effects of cybercrime. The role of law enforcement in investigating digital crimes is becoming increasingly important because of the rise in the number of digital crimes. The purpose of this research is to investigate the responsibilities that are necessary to combat cyber-crimes in the digital realm. With the help of this study, we hope to gain a better understanding of the role that law enforcement plays in protecting cyberspace from digital offences. This places an emphasis on understanding the legal framework, incorporating recommendations, and case study analysis to determine the factors that lead individuals to become victims of digital crimes.

Keywords: Digital Space, Cyber Crime, Information Technology Act, Law Enforcement.

INTRODUCTION

Fraud, theft, mischief, forgery, defamation, stealing, cyber harassment, and similar offences perpetrated via cyberspace (any electronic device) with the intent to cause substantial harm to others constitute digital crime. Increase of cybercrime has incentivized criminal activities, cyber criminals are being paid for stealing credit card information's, email accounts of individuals. The significance of cybercrime investigations and the role of law in regulation is paramount. A pertinent inquiry that arises now is how cyber policing is conducted.

The Information Technology Act of 2008 explicitly delineates Sections 78 and 80, which empower police officers to conduct searches, enter premises, inspect, and make arrests without a warrant if they possess reasonable suspicion of an offence being committed or about to be committed under the Act. The efficacy of digital crime investigations is contingent upon the officers overseeing them, necessitating the recruitment of the most qualified individuals in the field of cyber-crime technology to mitigate potential threats. The Supreme Court of India, in the case of *Prakash Singh and Ors. v. Union of India*, has mandated the establishment of specialised investigative police, distinct from law enforcement agencies, to facilitate more effective dispute resolution. Numerous legislations, including the *Model Police Act of 2006*, also stipulate such measures. It is essential that digital crimes are investigated comprehensively, necessitating a specialised team to effectively combat cyber-crimes in the digital realm.

²² Assistant Professor at IILM University, Gurgaon, India.

COMBATTING CYBER CRIMES

Indian legislation mandates cyber policing, which is essential for addressing cyber-crimes. “*Section 69 of the IT Act authorises the government and its agencies to intercept, monitor, or decrypt any information generated, transmitted, received, or stored in any computer resource, contingent upon adherence to the established procedures.*” This authority may be exercised if the Central or State Government considers it necessary or beneficial for the preservation of India's sovereignty or integrity, national defence, state security, diplomatic relations, public order, or to prevent incitement to any cognisable offence or for the investigation of any crime.

The “*Budapest Convention*,” which came into effect in 2004, addresses cyber-crimes in the international context and recommends the integration of safety mechanisms into the domestic laws of nations. Regrettably, the convention has not garnered international approval, and India has also dismissed it on the grounds that it was absent during the draughting process, which may infringe upon India's sovereignty.

Taking into consideration this convention, I believe it is of the utmost importance to recognise that the state is not the sole protector of cyber policing. Corporations and non-governmental organisations (NGOs) should be given the responsibility of addressing cybercrimes. These organisations should be able to obtain prior approval from the government to leverage their expertise in strengthening security mechanisms. This will result in the creation of an environment that supports justice and serves as a deterrent for individuals who commit such offences. Criminals who commit such offences may operate in several different jurisdictions, such as different countries. An international convention that is supported by the international community could serve as a norm that is legally binding to punish those who commit such offences.

CYBER CRIME INVESTIGATION

Given the rise in cyber-crimes, it is imperative to establish effective mechanisms, as investigation is crucial for holding perpetrators accountable for their offences. A functional model for cybercrime investigations is essential, and I believe it is necessary to integrate the following elements to combat cybercrime effectively.

To reduce the likelihood of cross-contamination, it is essential to have a thorough understanding of the procedures for gathering evidence and how it will be utilised, as well as the processes for storing evidence. In the case of recovering data that has been deleted, for example, the examination of evidence pertains to recover the data. To ensure that investigations into cybercrime are carried out without any interruptions and to guarantee that compliance is achieved, these methods need to be integrated.

CASE STUDY

The purpose of the case study is to bring attention to the fact that it is essential for individuals to increase their awareness of the cybercrimes that are currently occurring in our society. Because cybercrimes are

not limited by jurisdictional boundaries, it is imperative that efforts be made to cultivate an environment that is robust in terms of cyber security.

Case study – 1

The WannaCry Ransomware Attack: In 2017, a global cyber assault targeted systems running on Microsoft Windows, encrypting files and demanding a ransom for their release. The attack significantly affected over 100 countries and organisations, including Honda, FedEx, and Nissan. The solution was initiated by security researcher Marcus Hutchins, who released emergency security patches and collaborated with cybersecurity firms to eliminate the worm. Consequently, extensive systems that were impacted had to either pay a ransom to decrypt their files or await security patches to address the vulnerability.

It is essential to acknowledge that we were not adequately prepared to deal with this ransomware. For this reason, I believe that we require the assistance of cybersecurity companies that collaborate with the government and engage in cyber policing, which has the potential to reduce the severity of such impacts on a global scale. It is imperative that we take immediate action to bring about a change in our laws and integrate the work of cyber security firms with the work of the government.

Case Study - 2

Remote Access Trojan (“RAT”) A schoolteacher named Aisha inadvertently downloaded a malware Remote Access Trojan (“RAT”) onto her smartphone. The malware compromised Aisha's phone, granting the cybercriminal access to her email and text messages, which were subsequently disseminated to her colleagues and family members. The images were digitally manipulated (“deepfakes”) and uploaded to pornographic websites. This case highlights the necessity of promptly reporting such crimes to cyber security units; however, Aisha initially failed to report the incident to the police and instead attempted to trace the websites where the images were disseminated. The Australian Police subsequently acknowledged the case and resolved the issue.

Case Study 3 -

Yahoo Data Breach – The Yahoo data breach involved cyber attackers stealing user data from the platform, with the identity of the hackers remaining unknown to this day. The hackers appropriated data and subsequently sold it. The hackers compromised the platform's security and accessed all sensitive user information. These case studies provide insight into the expanse of cyberspace and underscore the necessity of raising awareness regarding the occurrence of such crimes, while also emphasising the imperative to investigate these offences by introducing innovative concepts and mandating the role of cyber police to take prompt action.

SUGGESTIONS

We are unable to address the challenges that are presented by cyber criminals, even though there are laws and international norms regarding this matter. Taking action to address these concerns is mandatory. I would like to make the following recommendations to improve the efficiency of cyber policing and counteract the problem of cybercrime.

- **Education:** The proliferation of technology has granted universal access to the internet and smartphones. For educational purposes, we have integrated technology into classrooms, and cyberspace is now utilised for financial, educational, and recreational activities. This serves as a reminder to educate all individuals about cyberspace. Instructing children and adults on the nature of cyberspace, as well as the laws and initiatives implemented to safeguard against cybercrimes. A mandatory curriculum should be implemented in educational institutions, and a mandatory training program should be implemented for professionals, to raise awareness about crimes of this nature and the importance of reporting them to the appropriate authorities.
- **Cyber Security Firms:** The government must collaborate with international cyber security firms, establish agreements such as Memoranda of Understanding, and grant them the autonomy to function as cyber law enforcement entities. Independent cybersecurity firms may receive pre-approval from governments, serving as the primary resource to assist law enforcement in fulfilling its responsibilities. Cybersecurity experts are essential, and such firms offer a reliable platform that the government can depend on. Granting this firm autonomy to operate within state regulations will enhance cybersecurity and improve the efficacy of cyber policing. Their role is critical, as evidenced by the “WannaCry Ransomware Attack,” in which a cybersecurity expert from a cyber firm proved valuable in resolving the issue.
- **Role of International Law:** International law must be enforced within the realm of cyberspace. The international community must confront the challenges posed by cybercrime and cyber policing. It is my belief that an international treaty is necessary, requiring ratification by members of the international community and implementation within their domestic legislations. The implementation of this measure would ensure that all cybercrimes that take place in any jurisdiction are dealt with in a consistent and fair manner. In addition, there is a need for the establishment of an independent international cyber tribunal to address potential trans jurisdictional issues and ensure that justice is maintained among member nations. In this court, individuals who have been harmed by cyber-crimes or crimes that have affected the country could file an independent case. Through this court, cyber experts can conduct comprehensive investigations and hold the perpetrators accountable for their actions. International law can play a pertinent role to bring about changes and the need is to create awareness and raise concerns for cyber security.
- **The necessity for victim support services:** Any cybercrime can adversely affect an individual's mental and emotional well-being. An immediate necessity exists to implement a victim support service mechanism for individuals affected by cybercrime. These centres can assist victims in overcoming emotional trauma and facilitate their reintegration while educating them about cybersecurity. These centres can be a driving force to help individuals going through emotional hardships faced due to cyber-crimes.
- **Cyber Police:** It is essential to recognise the necessity of an autonomous cyber policing framework. The Hon'ble Supreme Court of India has emphasised the necessity for an independent cyber policing unit that functions autonomously from the regular police force. To

differentiate between digital police and investigating officers and other law enforcement personnel, a distinction needs to be established. While a trained team needs to be established, a legal framework that mandates the formation of such a team would help reduce the number of cybercrimes and ensure that those responsible are held accountable.

CONCLUSION

There has been an increase in cybercrime because of the introduction of technology into everyday life and the digital realm. It is imperative that laws be put into effect and that awareness be raised at this very moment. If we are aware of the rights that we possess, how we can report crimes of this nature, and the measures that will be taken, then the fear of the people would reduce, if anyone committed such a crime. This is because they would have faith in the cyber policing mechanism and in the laws that are designed to punish those who commit such crimes. The digital space will present such challenges, and cybercriminals will take advantage of them. However, as individuals, we have a responsibility to keep ourselves informed about the initiatives taken by the government, to suggest that the government act, to file public interest litigations, and to seek justice and corrective measures from the court to reduce the number of crimes of this nature and to hold those responsible for offences of this nature accountable. In this context, the identification of data through cyber police becomes more important to check what crimes are being committed, as well as the number of crimes of this kind that are being committed using the same IP address, and to locate those responsible. Even though India has robust legislation in place to ensure that cyber criminals are held accountable for their actions, we still need to ensure that these laws are enforced and that we create an environment in which everyone is aware of their rights and cyber security.
