The Social Science Review
A Multidisciplinary Journal
ISSN: 2584-0789
(Open-Access, Peer-Reviewed, Refereed, Bi-Monthly, International e-Journal)
Homepage: www.tssreview.in

BOOK REVIEW
CYBER ECONOMIC CRIME IN INDIA

Sayantan Saha
Research Scholar, Department of Political Science, University of Kalyani, West Bengal, India

Corresponding Author: Sayantan Saha

CYBER ECONOMIC CRIME IN INDIA (2020), by Balsing Rajput , Springer International Publishing, ISBN- 978-3-030-44657-4, Paperback. Pages: 262.

This book contributes to the literature on cyber economic crime detection by offering an overview of cybercrime in India through an analysis of fifteen years of data and particular case studies from Mumbai. This book examines the criminal justice system's response to cyber economic crime, with a focus on integrated victim-centered methods of localised investigation. It also suggests new approaches to detection and prevention. It considers the hazards of cybercrime, national security, and technical risks to commercial and technological facilities. The following subjects were covered:

- The evolving cybercrime landscape.
- Cyber crime typology.
- The legal framework in India addresses economic crime.
- India's cyber security measures

Balsing Khandusing Kamal Rajput M. Tech., Ph.D., is a researcher, lecturer, and prominent officer of the Maharashtra State Police. He is an expert in both technical and strategic cybersecurity matters. He has firsthand experience building 51 cyber labs and 43 cyber police stations in Maharashtra State to investigate cybercrime. He has overseen the implementation of the Automatic Multimodal Biometric Identification System project. He travelled with India's cybersecurity delegations to Estonia in 2019 and Israel in 2016. He has worked in the Mumbai Police's economic offences unit and handled numerous sensitive cases.

The 2020 publication, Cyber Economic Crime in India, spans 262 pages. The book provides a comprehensive discussion about cyber-economic crime in India. Cybercrime has become a threat to today's business and financial transactions. This book divides its ten (10) chapters into four parts. First part: Introduction This part has a total of three chapters. Each chapter discusses numerous sub-topics. Crime has existed since the beginning of human society, evolving with the development of science and technology. Technology, particularly the internet, has enabled more sophisticated commission of traditional crimes.

The first chapter discusses the importance of technology in India. The importance of the internet has increased since then due to its influence. The communication system has improved, and information exchange has become easier. This book beautifully presents the subject of cyberspace. Information technology has good and bad sides, such as security breaches. This book's central theme is cyber-economic crime. This book reviews the role of the judiciary in countering cybercrime. This chapter

explains the development of the internet, which has emerged as the world's most significant technological achievement. The chapter also introduces the information society and cyberspace. Cyberspace has become a commonplace aspect of existence. It is now an essential component of the world in which we live. In this field, crime is also not an exception. Since the beginning of time, crime has been a problem for society due to the sheer presence of humans. However, antisocial elements are exploiting advanced technologies to perpetrate numerous crimes in cyberspace. For a variety of reasons, crimes are organized. In today's societies, greed and illegal financial gain are common motivations. We introduce the topic of cybercrime with a brief contextual statement. We present advancements in the internet, criminal activity, and the criminal justice system to aid readers in comprehending the book's setting. This chapter introduces the other crucial subjects, such as economics and cyber economic crime, to help readers better grasp the book's main idea.

The second chapter's title is "Changing Landscape of Crime in Cyberspace." This chapter provides a quick synopsis of the current situation in cybercrime. Cybercrime agents resemble hacktivists and organised gangs in their complexity. With the development of technology and the widespread use of the internet, criminal tactics are evolving. Advanced persistent threats and social engineering are two examples of crime vectors that are covered. We illustrate several parameters to provide a brief overview of the evolving landscape of cybercrime, which includes attack vectors, crime agents, and the most effective tools or methods for crime and targeting. The top new dangers are mentioned.

The third chapter in the book is titled "The Cyber economic Crime Criminological Research and Frameworks." This chapter explains the conceptual underpinnings of cyber economic crime. It clarifies the idea of cyber economic crime in the Indian context from a criminological standpoint. It evaluates numerous criminological research studies on cyber financial crime in India, the responses of the criminal justice system, and the effectiveness of the legal system. It tries to investigate theories of crime and the evolution of cyber economic crime in criminology. This chapter also covers the theoretical underpinnings of cyber financial crime, providing an explanation of the concept, the phenomenon, and the response of the criminal justice system. It charts the relationship between technology and cybercrime. This chapter also explains the analytical and methodological foundation for studying the system's efficacy.

The second part of the book, Understanding Phenomenon, is the title. This section consists of three chapters, from IV to VI. The author discusses cyber economic crime from India's viewpoint in the fourth chapter, delving into the definition of cybercrime, the evolution of cybercrime patterns, the global nature of crime, and the characteristics of its commission. This chapter provides a comprehensive understanding of the concept, evolution, and nature of cybercrime. Additionally, it clarifies cybercrime from an economic perspective. The article delves into the problem of cyber financial crime within the Indian context, providing further details on its nature, scope, victims, accused features, and typology.

Cyber economic Crime Typology is the title of the fifth chapter. We discuss the various types of cyber economic crime. Examples include credit card fraud, cryptocurrency scams, online game cheating, and identity theft. This chapter tries to classify cyber economic crime by examining the typology of cybercrime and explaining the theoretical background. The chapter describes several methods for categorising cybercrimes, including technological, criminological, psychological, and sociological approaches. We categorize cyber economic crimes based on the methods used, the amount of money gained from the crime, the type of criminals or threat agents, and the type of target or victim. We also consider the classification based on the function of technology and the extent of reliance on it. We cover the most common forms of crime in cyberspace, including ransomware, phishing, and credit/debit card fraud, in detail.

The sixth chapter is about emerging trends and patterns of cyber economic crimes. This chapter discusses various incidents related to cyber economic crimes. With an emphasis on Maharashtra and Mumbai, this chapter examines trends and patterns in cybercrime in India. The chapter highlights that cyber economic crimes account for 93% of cases filed in Mumbai, while they account for 66% in Maharashtra. Statistical

data from India, Maharashtra, and Mumbai, along with a comparative analysis of six major cities between 2002 and 2016, bolster the study.

Part Three of this book is titled "Reaction of System in Combating the CEC." The seventh chapter discusses the legal aspect of cyber economic crime. The chapter delves into the laws that India has in place to combat cyber financial crime. This chapter examines significant sections of the IT Act. This chapter provides an overview of the current legal framework in India for handling cyber-economic crime. We examine the Information Technology Act in detail with regards to cyber economic offences. Additional general laws enforced to deal with cyber economic crimes are considered, such as the Indian Evidence Act, Criminal Procedure Code, and Indian Penal Code. We also examine inadequate provisions in cyber economic crime legislation and relevant case laws. We analyse the complete investigation process to provide a concise overview of the criminal investigation procedure.

The eighth chapter, Criminal Justice Administration in India: An Overview, analyzes the functions of the judiciary in suppressing CEC and the role of the state police force in countering CEC in India. This chapter provides an overview of the numerous parties involved in the criminal justice system's response to cyber economic crime. We provide an overview of the functions of organisational structure, accountability, and human resources, along with a brief introduction, to help readers understand the roles that various components of the criminal justice system perform. British rule in India established the Criminal Justice Administration to ensure effective handling of criminal cases. It is the common law's adversarial system. We also cover a brief synopsis of the criminal justice systems in Mumbai and Maharashtra to enhance our understanding of the institutional structures at the state and local levels.

The ninth chapter highlights a unique aspect: the challenges and problems of the criminal justice system. This chapter's title is "The Response of the Criminal Justice System." This chapter examines the responses of several parties involved in cyber economic crime, including the judiciary, police, prosecutors, defence attorneys, and forensic labs, about their roles throughout the investigation and prosecution process. The chapter offers case studies highlighting cyber economic crime disposal, pendency, detection, and conviction rates. We also analyze the difficulties and issues that all parties face.

The fourth and last part of the book is titled The Way Forward for Combating CEC. The tenth chapter proposes an integrated cybercrime and cybersecurity model that focuses on proactively identifying threats, creating response mechanisms, and conducting investigations. It recommends the establishment of a National Cyber Agency (NCA) as the central coordinating body for threat analysis and prevention. Institutional arrangements for all stakeholders at different levels are considered, including separate wings, strengthening existing mechanisms, and creating an online mechanism. This chapter also discusses the importance of cyber literacy in preventing cybercrime and suggests initiating a digital literacy drive as part of the prevention framework. The tenth chapter's title is Integrated Cybercrime and Cyber Security Model. This chapter discusses the government's initiatives to combat cybercrime in detail. This section discusses the functions of the national cyber agency, the national cyber coordination center, and the state cyber crime coordination center. This chapter presents recommendations about the criminal justice system's (CJS) specialist institutional, legal, and awareness initiatives for combating cyber economic crimes. A new integrated cyber security model for these cybercrimes is being considered to effectively address the numerous difficulties and issues that different CJS stakeholders face. The model provides several frameworks for support, as well as implementation strategies. We advise different institutional and legislative structures and interventions to promptly and effectively respond to these cyber economic crimes, given that cybercrime is an international and cross-domain issue. We also advise using the newest technology to expedite the judicial and investigative processes.

Balsing Rajput's book, Cyber Economic Crime in India and an Integrated Model for Prevention and Investigation, beautifully discusses various topics, such as reviewing the causes of cyber economic crime. The book also discusses the role of the police and judiciary in preventing cyber-financial crime. The book also examines the laws associated with cybercrime. While the book discusses the legal aspects, it does not elaborate on the administration's strategy to counter the cyber economy. This book doesn't fully address

the challenges the police administration faces in combating cybercrime. The book does not explicitly discuss the limitations of the proposed integrated cybercrime and cybersecurity model. Overall, the book opens up new horizons in the discussion of cybercrime. The book is essential for researchers, legal advisors, and people associated with law enforcement.

References

1. Iqbal, J., & Beigh, B. M. (2017). Cybercrime in India: trends and challenges. *International Journal of Innovations & Advancement in Computer Science, 6*(12), 187-196.
2. Rajput, B. (2020). *Cyber Economic Crime in India*. Springer International Publishing.
3. Sarmah, A., Sarmah, R., & Baruah, A. J. (2017). A brief study on cyber crime and cyber laws of India. *International Research Journal of Engineering and Technology (IRJET), 4*(6), 1633-1640.
4. Sharma, V. (2011). *Information technology law and practice.* Universal Law Publishing.