# Chapter 50
# A Study of Cyber Crime and Perpetration of Cyber Crime in India

**Saurabh Mittal**
*Asia Pacific Institute of Management, India*

**Ashu Singh**
*Asia Pacific Institute of Management, India*

## ABSTRACT

*The world is facing a new era of criminal activities in cyber space, which are being committed across the world, irrespective of geographical boundaries. These cybercrime acts may be financially driven acts, related to computer content, or against the confidentiality, integrity, and accessibility of computer systems. The relative risk and threat differs between governments and businesses. The level of criminal organization represents a defining feature of the human association element behind criminal conduct. India accounts for close to $8bn of the total $110bn cost of global cyber crime. The Information Technology (IT) Act, 2000, specifies the acts that are punishable. Cyber crime has also affected the social media. A crime prevention plan with clear priorities and targets needs to be established, and government should include permanent guidelines in its programmes and structure for controlling crime and ensuring that clear responsibilities and goals exist within government for the organization of crime prevention. This chapter seeks to find out the motives and suspects of cyber crime perpetration and suggests measures for crime prevention.*

## INTRODUCTION

Cyber Crimes are a new class of crimes rapidly increasing due to extensive use of Internet and I.T. enabled services. Computer crime is one of the fastest-growing types of illegal activity, both in the U.S. and internationally. While the Internet links people together like never before, it also provides endless opportunity to criminals seeking to exploit the vulnerabilities of others. There are several different types of computer crime, many of which overlap. Below are a few of the most commonly reported cyber crimes:

DOI: 10.4018/978-1-5225-8897-9.ch050

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

- **Phishing:** Phishing is the practice of sending fraudulent emails in an attempt to trick the recipient, usually for the purpose of obtaining money. The elderly are particularly vulnerable to these types of cyber crime.
- **Hacking:** Hacking is similar to digital trespassing. Hackers infiltrate online networks to illegally download confidential information, manipulate functions and in some cases steal identities that can be used to fraudulently purchase goods online.
- **Stalking and/or Harassment:** Not all types of cyber crime involve money. Some cyber criminals use the Internet as a cover for other illegal behaviors like stalking, harassment and in lesser cases, bullying.

The Information Technology (IT) Act, 2000, specifies the acts which are punishable. Since the primary objective of this Act is to create an enabling environment for commercial use of I.T., certain specific omissions and commissions of criminals while using computers have not been included. Several offences having bearing on cyber arena are also registered under the appropriate sections of the IPC with the legal recognition of Electronic Records and the amendments made in several sections of the IPC vide IT Act, 2000.

## NATURE OF CYBERCRIME ACTS

Cybercrime acts may be financially-driven acts, related to computer content, or against the confidentiality, integrity and accessibility of computer systems. The relative risk and threat may vary between Governments and businesses. Individual cybercrime victimization is significantly higher than for ‘conventional’ crime forms especially in countries with lower levels of development, highlighting a need to strengthen prevention efforts in these countries. Private sector enterprises in Europe report victimization rates of between 2 and 16 percent for acts such as data breach due to intrusion or phishing. Criminal tools of choice for these crimes, such as botnets, have global reach. More than one million unique IP addresses globally functioned as command and control servers for botnets in 2011 (United Nations Office on Drugs and Crime, 2013).

- Internet content targeted for removal by governments includes child pornography and hate speech, but also defamation and government criticism, raising human rights law concerns in some cases.
- Some estimates place the total global proportion of internet traffic estimated to infringe copyright at almost 24 per cent.

## CYBERCRIME PERPETRATORS

Cybercrime perpetrators no longer require complex skills or techniques, due to the advent and ready availability of malware toolkits. Upwards of 80 per cent of cybercrime acts are estimated to originate in some form of organized activity, with cybercrime black markets established on a cycle of malware creation, computer infection, botnet management, harvesting of personal and financial data, data sale,

15 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/a-study-of-cyber-crime-and-perpetration-of-cyber-crime-in-india/228769

Related Content

Futurologist Predictions on Global World Order of Cyborgs and Robots
(2022). *Philosophical Issues of Human Cyborgization and the Necessity of Prolegomena on Cyborg Ethics (pp. 265-286).*
www.irma-international.org/chapter/futurologist-predictions-on-global-world-order-of-cyborgs-and-robots/291953

Navigating the Quandaries of Artificial Intelligence-Driven Mental Health Decision Support in Healthcare
Sagarika Mukhopadhaya, Akash Bag, Pooja Panwarand Varsha Malagi (2024). *Exploring the Ethical Implications of Generative AI (pp. 211-236).*
www.irma-international.org/chapter/navigating-the-quandaries-of-artificial-intelligence-driven-mental-health-decision-support-in-healthcare/343706

The Impact of Decentralized Technologies on Social Media Megacorporations
Richard Foster-Fletcherand Odilia Coi (2022). *Applied Ethics in a Digital World (pp. 140-156).*
www.irma-international.org/chapter/the-impact-of-decentralized-technologies-on-social-media-megacorporations/291438

The Human Factor: Cyber Security's Greatest Challenge
George Platsis (2019). *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications (pp. 1-19).*
www.irma-international.org/chapter/the-human-factor/228717

Cyber Security Operations Centre Concepts and Implementation
Enoch Agyepong, Yulia Cherdantseva, Philipp Reineckeand Pete Burnap (2020). *Modern Theories and Practices for Cyber Ethics and Security Compliance (pp. 88-104).*
www.irma-international.org/chapter/cyber-security-operations-centre-concepts-and-implementation/253664