Chapter 2
The Fundamentals of Digital Forensics and Cyber Law

Kirti Raj Raj Bhatele
BSF Academy, India

Deepak Dutt Mishra
BSF Academy, India

Himanshu Bhatt
BSF Academy, India

Karishma Das
BSF Academy, India

ABSTRACT

This chapter provides prerequisites associated with cyber crimes, cyber forensics, and law enforcement. It consists of a brief introduction to the definition of cyber crimes, its classification, challenges associated with it and how it evolved with time, impact on the society, cyber terrorism, and the extent of problem scalability along with focusing on law enforcement aspects associated with the tracking and the prevention from such type crimes. The aspects discussed here include various cyber laws and law enforcement techniques introduced by various countries throughout the world which helps them to fight against cyber crimes. The cyber laws discussed include Australian, Canadian, United States, United Kingdom, and Indian law. This chapter also deals with the digital/cyber forensics, what does digital/cyber forensics mean, its types, and laws/rules revolving around them, like how to collect evidence, jurisdictions, and e-discovery.

DOI: 10.4018/978-1-5225-8241-0.ch002

INTRODUCTION: CYBER CRIME

Cybercrimes are described as crimes committed using a computer network. It is illegal behaviour directed by means of any electronic operations. If taken exactly, each term suffers from one or more insufficient. Mainly cybercrimes or virtual crimes are may be seen as focusing exclusively on the Internet. The terms such as 'digital', 'electronic or 'high-tech' crime may be seen as so broad as to be meaningless.

For example, 'hi-tech crime' may go afar networked information technology to include other 'hi-tech' developments such as nanotechnology and bioengineering. Terms should not, however, be approached mainly, but rather as usually descriptive terms which importance the role of technology in the commission of a crime. Although it is still the case that no one term has become truly prevalent, with many being used interchangeably, 'cybercrime' has been adopted in this chapter for a number of reasons. First, it is mainly used in the literature. Secondly, it has found its way into common usage. Thirdly, it accents the importance of networked computers. Fourthly, and most importantly, it is the term adopted in the Council of Europe Convention on cybercrime.

Evolution of Cyber-Crime

All know that the radical change in transportation of persons and goods affected by the introduction of the automobile, the speed with which it moves, and the ease with which malevolent persons can avoid capture, has greatly encouraged and increased crimes. In 1920s automobile is equally opposite of digital technology today. There also have been negative aspects of these developments. The convenience and ease provided through electronic banking and online sales also form a ground for the commitment of frauds. Electronic communication such as email has helped us to communicate farther away it also has generated issues like stalking and harassment. Due to a greater need for computers and digital networks, we have grown entirely dependent on them. Technology has made itself a tempting target; either for the purpose of gaining important and various types of information or for the objective of causing disruption and damage (Clough, 2010).

The Challenges of Cybercrimes

The societies we live in nowadays have grown extremely dependent on science and technology, and ironically most of us don't know much about it. For the commission of a Cybercrime, there is a requirement of three factors: a motivated criminal or a group of motivated criminals, the presence of opportunities to perform the heist and absence of individuals who can prevent them from doing so. On the account