Chapter 4.1
A Comparison of Cyber-Crime Definitions in India and the United States

Himanshu Maheshwari
University of South Florida, USA

H.S. Hyman
University of South Florida, USA

Manish Agrawal
University of South Florida, USA

ABSTRACT

Unlike traditional crimes, it is difficult to define legal jurisdiction and authority for prosecuting cyber crimes. This issue is further complicated by differences in definitions of cyber crime in different countries. This chapter motivates the issue with an example of the ILOVEYOU virus and compares the legal provisions to combat cyber-crime in the US and India. The authors find that there are significant differences between India and the US in definitions of cybercrimes. It appears that in the United States, it is a crime to access information that has been declared to be confidential. In India, criminality requires dissemination of the information obtained without authorization. Another notable difference between the prosecutions of cybercrimes in the two countries relates to obscenity and decency laws.

INTRODUCTION

While most individuals and businesses use the Internet as a communication medium to learn and to socialize, other individuals and groups use the Internet as a medium for criminal purposes. The Internet has positively transformed many legitimate business activities, lowering costs and accelerating transaction speed. It has also served as a platform for criminals who strategize online and attack valuable targets at a remote distance from the crime scene. (Phil Williams)

Successful investigation, apprehension and prosecution of cyber-crime require an extension of existing attitudes and assumptions of legal boundaries, and methods used by law enforce-

DOI: 10.4018/978-1-61350-323-2.ch4.1

ment to solve crimes. One traditional assumption associated with investigating crime is the physical proximity of victim and perpetrator. Many personal crimes occur face to face, such as robbery or assault. Property crimes such as burglaries and thefts occur locally and the perpetrators are usually, but not always, present at the scene of the crime.

Some exceptions to this usual occurrence are instances of conspiracy, and principal theory; both provide for prosecution of participants to a crime, who may not be present at the time of its occurrence. Perpetrators of cybercrime, by the very nature of the offences committed, are located remotely, and quite often in other countries, where it is difficult to determine legal jurisdiction. Which country has the authority to prosecute? Is it the country of the victim or the defendant? Where did the crime actually take place?

By now many readers are familiar with scams originating in Nigeria, in which the criminal claims to have access to millions of dollars, and all that is needed from the victim is a few thousand dollars to pay the transfer taxes. If a person from Nigeria sends an email to an individual in the United States, requesting money and the individual sends the money to Canada, where did the crime take place, in one, two, or all three countries?

Remotely perpetrated financial scams are not new phenomena. There are many laws and agencies in the United States specifically mandated to target crimes such as wire fraud (18 USC 1343, mail fraud (18 USC, Chapter 63), and money laundering (Bank Secrecy Act of 1970, Patriot Act of 2001). However, resources now must consider the impact of crimes that are launched from remote locations far beyond the borders of the victim country. For example, the Love Bug virus, which was launched from the Philippines in 2000, caused damage to computers in more than twenty countries, causing damage estimated to be in the billions of dollars. As described later in the paper, the perpetrators were caught in no time, but authorities could do little to prosecute them because of weaknesses in cybercrime laws.

Definitions of cybercrime are not uniform across countries, so behavior legally defined as a crime in the victim's country may not be defined as such in the perpetrator's country. For example, while it was relatively easy for US agencies to trace the origins of the ILOVEYOU virus to an apartment in Manila in the Philippines. Prosecution was another matter because at the time of the offense, no law existed in The Philippines that made this behaviour illegal. The behaviour in this case was the creation of a software virus.

In discussing cybercrime, it becomes necessary to begin with a clear listing of cybercrimes defined within each jurisdiction. This paper examines the definitions of cybercrimes in India and the United States. We draw upon the US Code and the Indian IT Act. The paper is organized as follows we begin with an introduction to cybercrime, cyber law and cyber forensics we then report current statistics on reported cybercrime. This is followed by a comparison of legal provisions to help prosecute cybercrime in India and the United States.

CYBER CRIME

Cybercrime is defined as crimes committed on the Internet using the computer either as a tool or a targeted victim. However, some overlap occurs in many cases and it is difficult to have a clear cut classification system. We breakdown cybercrime along two dimensions. The first dimension the computer as a tool and as a target. The second dimension is the classification of crime itself: Person, Property, and Victimless/Vice.

In our first dimension, we divide cybercrime between the following two categories:

a. Using the computer as a tool: In this case, the target of the cybercrime is an individual. Such crimes usually do not require a high level of technical expertise; the target is somebody in the real world. The objective is to attack a person in a very subtle manner