Chapter 5.2
Definition, Typology and Patterns of Victimization

Debarati Halder
Centre for Cyber Victim Counselling, India

K. Jaishankar
Manonmaniam Sundaranar University, India

CHAPTER OVERVIEW

In this chapter, an attempt is made to operationally define cyber crimes against women, as we have found that the definitions of cyber crimes have changed in the past decade and we presume that even this will change in the future decades to come. In addition, the current definitions do not specifically fit in to the nitty-gritty issues of cyber crimes against women and a succinct operational definition is provided. A new set of typology is made with regard to the cyber crimes against women as not all type of crimes fit to the category of cyber crimes against women. The patterns of victimization of women in cyberspace are dealt by qualitative case studies along with the typology.

INTRODUCTION

Post world wars, many had been victimized by different types of crimes including war crimes, terrorism, human rights violations, economic crimes etc. Later, with the advancement of telecommunication technologies in post 60's, victimization by the ugly side of technology such as cyber crime occurred. During the initial period of the occurrence, the term "Cyber Crime" was never defined by any legal provisions, Bills, draft laws or conventions. It had been more an effort by the academicians and computer specialists to define and analyze the term "cyber crime" from the perspectives of (i) attack on the "machine" and (ii) computer assisted crimes (Wall, 2005, revised in 2010; Katyal, 2001)

The US Department of Justice (1989), defined computer crimes as "those crimes where knowledge of a computer system is essential to commit the crime" (Parker, 1989, p. 22). According to the report prepared by McConnell International (2000,

DOI: 10.4018/978-1-61350-323-2.ch5.2

p. 1), cyber crimes are, “harmful acts committed from or against a computer or network”. Katyal (2001, p. 12-13) suggests that “computer crime can be explained as the crime where the computer is used to carry out or facilitate a criminal offence either (i) by electronically attacking the computer as a machine, or (ii) by using the computer to commit a traditional crime”. In the first case, cyber crime can happen when computer files and computer programmes are unauthorisedly accessed (Katyal, 2001), or these files or computer programmes are unauthorisedly disrupted, or when electronic identity is stolen (Katyal, 2001). In the second case, cyber crime can happen when computer is used as a device to commit traditional crimes (Katyal, 2001) like creating or distributing child pornography, or carrying on some white collar crimes like insurance frauds or copying popular copyrighted songs and thereby violating the copyrights of the song etc. Nonetheless, these definitions show that the term “cyber crime” carries a connotation of any crime done with cyber assistance.

The definition of cyber crime got a facelift by the creation of Convention on Cyber Crime of Council of Europe, presented at a meeting held at Budapest, Hungary, in 2001. The Convention on Cyber Crime (2001) is the first of its kind which tried to look at the concept of ‘cyber crime’ from a global angle. This convention presented the concept of cyber offences in five dimensions. They are (i) offences against the confidentiality, integrity and availability of computer data and systems; (ii) Computer related offences; (iii) content related offences; (iv) offences related to infringements of copyright; (v) abetting or aiding such offences (Council of Europe, 2001).

The first group, i.e., offences against the confidentiality, integrity and availability of computer data and systems included the following:

(a) Intentional illegal access to the whole or any part of the computer system by infringing security measures. The motive could be either to obtain computer data, or any other dishonest intention, or illegal access in relation to a computer system that is connected to another computer;

(b) Intentional illegal interception without any proper rights whatsoever, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data;

(c) Intentionally interfering with the data without any proper rights what so ever;

(d) System interference, i.e., hindering of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data;

(e) Misuse of devices; this includes the production, sale, procurement for use, import, distribution of a computer device or programme designed or adapted primarily for the purposes of offences mentioned above under point (a) or a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, and the possession of any of these items with a criminal intent (Council of Europe, 2001).

The second group, i.e. ‘Computer related offences’ would mean:

(a) computer related forgery i.e., the input, alteration, deletion, or suppression of computer data resulting in inauthentic data with the intent that it may be acted upon for legal purposes as if it were authentic for fraudulent purposes; and

(b) computer related fraud, i.e., intentionally causing of a loss of property to another person by either (1) any input, alteration, deletion or suppression of computer data, or (2) any interference with the functioning of a computer system, or both with fraudulent