Chapter XXXVII
Cyber-Victimization

Lynne D. Roberts
Curtin University of Technology, Australia

ABSTRACT

Information and communication technologies (ICTs); while providing a range of benefits to individuals, organisations and governments; also provide new opportunities for criminal activities to emerge. This chapter provides an overview of criminal victimization online. The focus is on the impact of cyber-crimes on victims and the associated legal, technical, educational and professional responses to cyber-victimization. The focus on cyber-victimization is situated within the broader context of responses to victims of crime in off-line settings. The form of cyber-crimes will continue to change as new ICTs and applications emerge. Continued research into the prevalence, types and impacts of cyber-victimization is required in order to inform victim service provision and effectively address the needs of current and future cyber-victims.

INTRODUCTION

The use of information and communication technologies (ICTs) is ubiquitous in western societies. Networked computers enable instantaneous global communication and transfer of digital information. The introduction of third generation (3G) mobile telephones provides the potential for wide-spread mobile Internet access. Networked ICTs provide social, educational, information, personal and financial opportunities. However, these same technologies also create new opportunities for criminal activity. Networked computers provide the media for new types (or variations on old types) of criminal activity to emerge. The introduction of each new information and communication technology (ICT) potentially expands the range of criminal opportunities and potential victims. While these 'cyber-crimes' have received considerable media and some academic attention, the focus has largely been on the crime rather than offenders or victims (Wall, 2005). Limited research has specifically examined cyber-crime from the perspective of the victim.

This chapter provides an overview of the current state of knowledge on cyber-victimization. It begins with a brief overview of cyber-crime, delineating cyber-crimes 'against property' and

cyber-crimes 'against the person'. Six types of cyber-crimes are examined in terms of their defining features and prevalence. The body of the chapter examines the impact of personal and property cyber-crimes on victims with a focus on organizations, adults and children. Current legal and law enforcement, technical, educational and professional responses to cyber-victims are outlined. The examination of responses to cyber-victimization is situated within the broader context of responses to victims of crime occurring outside the virtual arena. The chapter ends with an acknowledgement that the continued development of ICTs will result in the emergence of new types of cyber-crimes and associated cyber-victimization. Continued research into the impacts of cyber-victimization is required in order to effectively address the needs of current and future cyber-victims.

BACKGROUND

ICTs may be used as a means of communication and organization to support criminal activities. ICTs provide criminals with a "global reach" (Savona & Mignone, 2004, p. 5) through cheap, fast, secure, anonymous communication with multimedia capacity. Further, ICTs can create new opportunities for criminal activity and provide new ways of conducting existing criminal activities (Savona & Mignone, 2004; Wall 2005).

These criminal activities that are enabled by ICTs are broadly referred to in the media and some academic discourse as cyber-crime. While the use of the term cyber-crime has been criticized as being "fairly meaningless because it tends to be used emotively rather than scientifically … with no specific reference point in law" (Wall, 2005, p. 79), it provides a useful umbrella when considering crimes committed using ICTs.

Competing definitions of cyber-crime have emerged. For example, Tavani (2004) argued for limiting the use of the term to only those crimes "in which the criminal act can be carried out only through the use of cybertechnology and can take place only in the cyberrealm" (p. 183). Tavani delimited cyber-crime from 'cyberrelated crimes' which include 'cyberexacerbated crimes' (such as cyber-stalking, online paedophilia and Internet pornography where technology can affect the scope of the crime) and 'cyberassisted crimes' (such as using the Internet to lodge fraudulent income tax forms) where the technology is used to assist in the conduct of the crime without affecting the scope of the crime. Similarly, Grabosky (2004) differentiated between conventional crimes committed with computers from cyber-crimes that involve attacks on computer networks, including theft and espionage.

Wall (2005) proposed the use of an 'elimination test' to determine whether a crime would still exist without the Internet. Using this elimination test Wall concluded that the Internet provides increased opportunities for existing types of crime (without the Internet these crimes would still exist, but would likely be reduced in number), new methods of conducting traditional crimes (without the Internet these new opportunities for offending would disappear) and opportunities for conducting new types of criminal activity.

Within definitions of cyber-crime, differing typologies of cyber-crimes have been developed. For example, Gordon and Ford (2006) differentiated between cyber-crimes that are single, discrete events facilitated by crimeware programs and exploiting system vulnerabilities (e.g. phishing, hacking and identity theft) and cyber-crimes that involve repeated contacts or events and that typically do not depend upon crimeware programs (e.g. cyber-stalking, child predation and cyber-extortion). Wall (forth-coming) differentiated between computer integrity crimes (e.g. hacking, denial-of-service attacks and viruses), computer related crimes that use networked computers to conduct criminal activities (e.g. cyber-piracy) and computer content crimes where illegal materials,