Chapter 7.5
Emerging Cybercrime Variants in the Socio-Technical Space

Wilson Huang
Valdosta State University, USA

Shun-Yung Kevin Wang
Florida State University, USA

ABSTRACT

This chapter examines the gaps that arise between reactive social control systems and proactive technology systems. The authors further link these gaps to cybercrime patterns and growth, by a theoretical framework that depicts the role that cybercrime plays in different gaps. This further suggests a typology of cybercrime, based on instrumental vs. expressive differences between offenses. Recent and emerging criminal activities and formal and informal control responses are reviewed and evaluated to illustrate this cybercrime framework and typology. The result is proactive strategies that can help prevent cybercrime from occurring in the disjoints between social and technical systems.

The world has become too dynamic, complex and diversified, too cross-linked by the global immediacies of modern communication, for stability of thought or dependability of behaviour to be successful.

—Timothy Leary (1920-1996).

DOI: 10.4018/978-1-60566-264-0.ch014

INTRODUCTION

The advent of the Internet has undoubtedly revolutionized the way we work, communicate, entertain, learn, and think in the physical world. The Internet and its associated technology have created numerous, unprecedented forms of human interaction in a new, virtually constructed space, known as **cyberspace**. This social cyber milieu is invisible and intangible, but like oxygen, we know it exists in the human community (Rho, 2007). Relying on the Internet's interconnected computer networks, users can practically transmit information to one or countless recipients any time of the day or night over continents without physical constraints. This unbounded ability to communicate has created virtually limitless opportunities for innovators, resulting in new ways of human relations and interactions expressed in a variety of forms.

Yet like most innovations which have a tendency to crime (Merton, 1968), the Internet holds potential for misuse and abuse of information in human interactions. Crimes committed on or through the Internet, so-called **cybercrime**, are common and

indeed soaring (Cisco, 2007). A survey of computer security officials discovered that about half of responding companies experienced increased numbers of security incidents between 2004 and 2006 (Computer Security Institute, 2007). The survey further showed that as the incidents of cybercrime increased, the financial losses caused by these crimes escalated as well. These facts attest to the rising severity of crime resulting from the social system's inability to match the rapidly progressing technical system. How is this mismatch between the social and technical systems formed? How has cybercrime grown and expanded in this gap between the two systems? Finding answers to these questions is an important step in combating cybercrime and in some way helping to achieve a balance between the social and technical systems.

This chapter attempts to examine the evolution and growth of cybercrime in the gaps existing in the socio technical space. The chapter starts with a conceptualization of cybercrime and the creation of a classification scheme. The classification explains the role that information plays in variations of cybercrime. Next, a framework is introduced to depict how types of cybercrime have evolved in the socio-technical space. Recent cybercriminal activities are evaluated to illustrate the framework. Social responses in terms of formal and informal controls are also examined to assess their effectiveness in cybercrime mitigation. The main purpose of the analyses is to identify strategies which can better control crimes already active on the information superhighway and prevent the emergence of new variants of cybercrime.

DEFINING CYBERCRIME

The term cybercrime can be defined in a variety of ways depending on the perspective from which research is taken. The prefix "cyber" in Greek refers to navigation (Pangaro, 1991). Literally, cyber techniques are an art of steersmanship (Guilbaud, 1959). The cybernetics literature has built the foundation for the notion of a cyber system (Parsegian, 1972). In this cybernetic frame of reference, complex systems of technology, sociology, biology, psychology, communication, and many other fields can be combined to explain interconnectedness of human and machine. Cybercrime, as a member of the interrelated network, is thus confounded with numerous elements in the social and technical systems.

From a sociological point of view, cybercrime is not different from other types of crime. (Emanuelsson-Korsell & Söderman, 2001). Both are crimes of opportunity committed by a motivated offender against a suitable target under an unguarded condition (Cohen & Felson, 1979). However, cybercrime is also a technology offense. As Brenner (2007:386) stated, it is "the use of computer technology to commit crime." Because of the continuous breakthroughs in Internet technology, cybercrime can evolve into a new generation of criminal acts unseen and inexperienced. In this chapter, we take into account the socio technical aspects of cybercrime, and define it as a law violation involving abuse or misuse of information explicitly on or through the Internet. The specific function that information plays in a cybercrime can determine the nature and type of the illegal act. For instance, a 1994 report published by the U.S. Department of Justice included the following three categories of **digital crimes**: information as contraband, information as an instrumentality, and information as evidence (Casey, 2004). In this classification, a cybercrime is investigated based on the presence or absence of contraband information (e.g., an encryption software), information means (e.g., virus codes), and records of information (e.g., Internet access logs). A study by Emanuelsson-Korsell & Söderman (2001) focused on five types of information-technology crimes: computer viruses, unlawful access to computer systems, manipulation of data, theft of information, and fraud. Criteria relating to abused data or financial gains were employed to classify these