Chapter 36
Considering the Role of E–Government in Cybercrime Awareness and Prevention: Toward a Theoretical Research Program for the 21st Century

J. Mitchell Miller
University of Texas at San Antonio, USA

George E. Higgins
University of Louisville, USA

Kristina M. Lopez
University of Texas at San Antonio, USA

ABSTRACT
Cybercrime has exponentially increased in recent years as an unavoidable byproduct of greater internet use, generally, and presents a wide range of criminal threats to large companies and individuals alike. While cyber offenses (e.g., cyberharassment, cyberstalking, identity theft, and intellectual property theft) and their address have been examined across diverse academic disciplines including criminology, electrical engineering, sociology, and computer science, minimal consideration has been given to the role of e-government in combating cybercrime – a somewhat ironic oversight given the computerized context of both. After reviewing the nature of cybercrime, this chapter considers e-government policies addressing cybercrime awareness, prevention, and victimization services. Discussion centers on the prospects for cybercrime theoretical research program development toward best practices public policy.

DOI: 10.4018/978-1-4666-2136-7.ch036
INTRODUCTION

Internet use is now normative daily practice in multiple life spheres at individual, group, institutional, and societal levels. The computerization of North America, Europe, and much of the rest of the world has vastly modified, and in many respects improved (e.g., speed and efficiency), the nature of interpersonal communication, information dissemination, and business transactions. Innovation rarely transpires, however, without unintended consequences. In the ease of computerization, proliferated internet use has been coupled with new types of high tech computer crime threats that have redefined the nature of victimization and crime prevention.

Computer crime, conventionally referred to as cybercrime, regularly occurs in the virtual reality of cyberspace. Cybercrime typically involves illegal access to an information technology infrastructure and one or more of the following activities: illegal interception of data transfers, data disruption (e.g., intentional modification or deletion), electronic fraud, and/or forgery through identity theft (Higgins, 2009; Higgins, 2008; Douglas & Loader, 2000). These activities manifest in a variety of specific criminal offenses, both new types of crime inherent to virtual reality and traditional offenses facilitated by technology, that raise broad public policy issues and specific criminal justice system challenges.

The purpose of this chapter is to consider the role of e-government in addressing the growing and ever-evolving problem of cybercrime. After reviewing the extent and diversity of cybercrime, the government response, generally, and the role of e-government, primarily in American context, is observed. Discussion themes include an expanded e-government role necessary to meet current and future cyber-threats and advocacy for a research-based and best-practices public policy orientation. Accordingly, suggestions are provided for engaging a theoretical research program (TRP) facilitative of leveraging collective efficacy through virtual reality toward cybercrime reduction.

A BRIEF OVERVIEW OF CYBERCRIME

Cybercrime refers to a fairly broad range of criminal activities that can be generally dichotomized into acts that either attack individual central processing units or computer networks (e.g., malware and viruses) or utilize computer networks to engage crime (e.g., bulk email scams, identity theft, fraud, and cyberstalking). There are several aspects of deviant computer practices with criminal intent distinguishable by an offense-specific jargon that has permeated the popular culture. Spam, unsolicited and predatory bulk emailing that, although for genuine commercial purposes, violated numerous federal and international privacy, morality, and telecommunications acts (Wikipedia, 2009 E-mail spam legislation by country). Zombies are computers attached to and hijacked through the web that aggressively and resiliently randomly attack other machines. Hackers (i.e., cybercriminals) use internet connections to place a computer virus that regenerates without permission and compromises a computer’s ability to function regularly.

The everyday use of the term computer virus has become a “catch-all” reference for malware generally, including worms, Trojan horses, adware, and spyware. Bulk email scams are widely known as phishing, an attempt to acquire personal financial information through communications disguised as being from a trustworthy or reputable source. These problems are spread across computers through emails, accessing internet sites, and through shared DVDs and floppy disks. Thus, problems are rarely contained to a single machine. Collections of compromised machines (the zombies) are called a botnet that, in turn, control multiple affected linked machines remotely by a bot herder, a head hacker.