University of Cincinnati

Date: 2/21/2011

I, James W Carter II, hereby submit this original work as part of the requirements for the degree of Doctor of Philosophy in Criminal Justice.

It is entitled:

Local Law Enforcement in the Realm of Cyberspace: The Role of Local Law Enforcement Agencies in Controlling Internet Crime

Student's name: **James W Carter II**

This work and its defense approved by:

Committee chair: Lawrence Travis, PhD

Committee member: William R. King, PhD

Committee member: Bonnie Sue Fisher, PhD

Committee member: James Frank, PhD

1351

Local Law Enforcement in the Realm of Cyberspace: The role of local law enforcement agencies in controlling internet crime

A dissertation submitted to the

Graduate School

of the University of Cincinnati

in partial fulfillment of the

requirements for the degree of

Doctor of Philosophy

in the School of Criminal Justice

of the College of Education, Criminal Justice, and Human Services

by

James W. Carter II
M.S. Marshall University, 1997

Committee Chair: Lawrence F. Travis III, PhD

Abstract

Since at least the 1970's there has been speculation about the impact that the development of the internet would have on both the pro-social and the antisocial elements of society. Some authors have speculated that the nature of crime and the rates of crime are likely to change as a result of the ongoing technological revolution. Furthermore, it has been speculated that the technological revolution would affect the role of the police, as well.

The present study examines both the preferred and the enacted roles of local law enforcement agencies within the realm of cyberspace. The preferred role of the police was operationalized as the number of complaints an agency received during the 2006 calendar year concerning 20 different types of internet crime. The enacted role of the police was operationalized as the Overall Activity Scale, a summative index representing the number of activities in which an agency reportedly engaging in efforts to control internet crimes. The present study also examined the ability of the tenets of contingency theory to explain the enacted role of local law enforcement agencies as a function of the number of internet crime complaints received.

Data for the present study were gathered via self-administered questionnaires mailed to the chief administrators of 871 local law enforcement agencies in the state of Ohio. These agencies included 783 municipal police departments and 88 county sheriff agencies. While the response rate for the current study was only 17%, the findings begin the process of examining the role of local law enforcement agencies in policing cyberspace.

The findings of the present study suggested that a majority of police agencies in the responding sample did in fact receive complaints concerning internet crimes. Furthermore, the study found that the overall levels of activity of local law enforcement agencies in the responding sample were not explained by the number of internet crime complaints received. A multivariate regression analysis was largely un-interpretable due to problems of multicollinearity between the independent variables. However; one independent variable did emerge as a significant predictor of agency scores on the Overall Activity Scale.

Acknowledgements

There were so many people who made this project possible. Just in case, I miss one of you, let me just say "THANK YOU" to every single one of you. You know who you are and you know what role you played in this project.

First and foremost, I would like to thank my committee chairperson, Dr. Lawrence F. Travis III, for your assistance in turning a vague and ill-formed idea into a series of working researching questions. Also, without your many email reminders that the "clock is ticking" I would never have stayed on track. Thank you for all that you have done for me in the years that I have been at University of Cincinnati. I know it took me longer than most, but I did it…with YOUR help. I will make sure that you never regret that. Again, thank you.

I would also like to thank the members of my dissertation committee: Dr. James Frank, Dr. Bonnie Fisher and Dr. William King. When you agreed to serve on my committee I am sure that you never thought it would take me this long to finish it. Thank you for taking to time to share your wisdom and experience with me. Also, thank you for your willingness to do those last minute readings of my submissions. As impossible as this project seemed at times, I have to say that it was truly one of the most valuable learning experiences of my academic career—largely because of the lessons that each of you taught me. Thank you.

I would like to thank my wonderful wife, Lynn. The question is how do I even begin to express my thanks to you. You were the first person I met at UC and since that time you have been my loudest cheerleader, my strongest supporter, my best friend, my soul mate and my hero. Without you in my corner, I could never have done any of this. This project is as much yours as it is mine. It does not begin to say all that I feel, but thank you and I love you!

Finally, I would like to thank all the family and friends that supported me throughout this

process. Especially, I would like to thank my mother, Ada. You taught me the value of education and have always encouraged my academic career. I would also like to offer a posthumous thank you to my stepfather, Robert, who passed away in 2001. Your path was not one of formal education, but you seemed to always get accomplished those things that needed to get accomplished. Yours was often the voice of reason when I needed to hear it. I only wish that you could have seen the completion of this project. I would also like extend a thank you to Judy Little at Marshall University, whom I forgot to include last time. You have always been my a second mother to me and you've been my long distance cheerleader and contributed to my success in ways that you could not possibly imagine. Thanks, Judy for everything.

Again, if I have missed anyone please know that I do value and acknowledge the contributions you have made to my success. You might not be named, but know that you are appreciated.

Table of Contents

List of Figures and Tables

Local Law Enforcement in the Realm of Cyberspace:

The role of local law enforcement agencies in controlling internet crime

Chapter One: Problem Statement

Introduction

This dissertation takes the first step towards rectifying a significant oversight in the policing literature. Despite a dramatic growth in the popularity of cyberspace as an arena of academic study (Chatterjee, 2001), and a great deal of speculation by futurist scholars suggesting that the development of the internet and internet crime would have lasting effects on the nature of policing in America, surprisingly little scholarly attention has been devoted to studying the role of local law enforcement agencies in controlling internet crime.

The lack of scholarly attention devoted to examining the role local law enforcement agencies serve in controlling internet crime is especially surprising considering the number of Americans at risk of being victims of internet crime. Studies of computer ownership and internet usage suggest that nearly three-fourths of the American population currently access the internet. These estimates climb as high as 90% when limited to children, teens and young adults (Fox, 2005).

While many of the activities users engage in while online are relatively mundane and may carry little risk of victimization, other activities, such as making online purchases, open users to the possibility of being victims of internet crime. For example, according to ComScore, which maintains databases for tracking internet trends and usage, during the 12 days leading up to Christmas Day, 2006, Americans purchased more than $25,000,000,000 in goods and services online (Gardner, 2007). With so many internet users, and such large amounts of funds being transferred electronically via the internet, it is quite surprising that scholars have devoted so little

attention to studying the means by which local law enforcement agencies control various forms internet crime.

Furthermore, recent estimates of the costs of internet crime (both in terms of physical damage to computer systems and in terms of recovery from such crimes) suggest that such crimes are extremely costly to victims. For example, a recent survey by the Computer Security Institute and the FBI, estimated the financial losses suffered by businesses, in 2006, to be nearly $52,500,000 (Gordon et al., 2006, p. 15). Of this estimate, over half of the losses suffered was attributable to computer viruses (accounting for over $15,500,000 in loss) and was due to theft, destruction and corruption of information (accounting for over $10,500,000) by computer hackers gaining access to the information without authorization (Gordon et al., 2006, p. 15).

As a result of the above oversight, scholars are unable to articulate the current role of local law enforcement agencies in controlling internet crime. Specifically, very little is known about the volume of internet crime complaints local law enforcement agencies receive, the activities in which local law enforcement agencies engage in controlling internet crimes, or the extent to which crime control activities of local law enforcement agencies are correlated with the volume of internet crime complaints received. The current study seeks to articulate the current role local law enforcement agencies serve in controlling internet crime. Furthermore, the current study examines the extent to which various characteristics of local law enforcement agencies explain any observed variation in the role local law enforcement agencies serve in controlling internet crime.

In The Midst of a Revolution

Since shortly after the end of World War II, America has been in the midst of a technological revolution of "extraordinary proportions and far-reaching implications" (Toffler

and Toffler, 1995; Castells, 1985, p. 7). The pre-World War II industrialized society in which brawn was the most valued commodity is transforming into a society driven by information, valuing technological development and the accumulation of knowledge and skills (Toffler and Toffler, 1995). Within the developing information society, the number of "muscle jobs", the foundation upon which the pre-World War II society had been built, is decreasing while the number of white collar positions is increasing, as is the level of technological skill needed by those filling such positions (Toffler and Toffler, 1995). Employers are no longer willing to train newly hired employees, instead it is assumed that new employees will have the technical training and education needed to succeed in the workplace prior to being hired (Toffler and Toffler, 1995). Due to these continued changes in the workplace environment, knowledge and information are becoming two of the most valued commodities in *New America* (Toffler and Toffler, 1995). This developing focus on brain over brawn is evident in the rising level of educational attainment and literacy rates as workers adapt to societal and economic changes (Castells, 1985).

Throughout the ongoing technological revolution, modern America has been bombarded by a flood of technological advances, innovations and inventions (Massey, 1985). These new forms of technology are societal creations; and, as such, these technological developments have been influenced by the characteristics of the society creating them (Castells, 1985; Massey, 1985). The technological advances developed during the last half of the 20th century share two characteristics of *New America* (Castells, 1985; Toffler and Toffler, 1995). First, technology developed during the technological revolution has primarily been broad reaching process-oriented advances in the effective and efficient use of information to enhance performance and productivity (Castells, 1985). Second, the technology developed during the technological

revolution has focused on improving the production and use of information (Castells, 1985).

In no other fields are these characteristics demonstrated more succinctly than in the fields of computers and computer networks. Since the 1950's, researchers in the field of computing have designed and built computers that are considerably smaller (even portable), much more powerful, less expensive, and more efficient. These developments have allowed computers to penetrate virtually every aspect of society. However, the development of one technological advance in the field of computer networking has influenced how millions of Americans search for, gather and use information. During the last half of the 20th Century, the world saw major developments in the field of computer networking, the development of the first large scale computer networks. The creation of these networks paved the way for the development of two of the greatest technological developments of the 20th century—the Internet and the World Wide Web.

The Origins of the Internet and the World Wide Web

The Internet began as an idea in a series of memoranda written in the 1960's, in which J.C.R. Licklider discussed the creation of a massive computer network over which users from all over the world could share the costs of computing and allow users to access data sets and other resources without concern for geographic distances (Castell, 2001; Kovacich and Boni, 2000; Leiner et al., 1997; Abbate, 1999). The predecessor of the internet, a large scale computer network called ARPAnet, created in the early 1970's was an experiment by the Defense Advanced Research Projects Agency funded by the U.S. Department of Defense (Abbate, 1999; Leiner et al., 1997). Over the course of the next twenty years, the physical structure of the Internet grew and developed as researchers experimented with new techniques, hardware and applications. The population of network users grew with the development of the first desktop

computers in the 1980's, and increased further as access was opened to new segments of society including college students and commercial users.

Early in the 1990's, Tim Berners-Lee, an English high-energy physicist working for the Conseil Européen pour la Recherche Nucléaire[1] in Geneva, Switzerland, re-invented the Internet when he developed a new system for organizing, storing and retrieving documents via the internet. Berners-Lee's system, the World Wide Web (WWW), was designed around two principles. First, the World Wide Web relied on universal compatibility of documents (Berners-Lee, 1996). In other words, a document created by any computer and available via the World Wide Web had to be accessible and readable by any other computer regardless of the compatibility of the two systems (Berners-Lee, 1996). Second, Berners-Lee's system relied on the ability to link any two documents or resources via hyper-text links, thus creating a web of documents spanning the internet (Berners-Lee, 1996). In 1991, internet users could download the first web-browser program at no cost via the CERN web server (Berners-Lee, 1996). The release of the first web-browser program introduced the world to a user-friendly means of accessing material via the internet which mimicked human logic and thought processes (Berners-Lee, 1996). The success of the World Wide Web is best demonstrated by the measures of growth in its use over the first three years, when the load on the World Wide Web server grew by a multiple of 10 each year (Berners-Lee, 1996).

Today, the internet is used by millions of Americans. In 2000, only 37% of the adult population in America went online on a typical day (Rainie et al., 2006, p. 58). By 2004, that percentage had risen to include 63% of adult Americans (Rainie et al., 2006, p. 58). Some of the latest studies indicate that in 2006, nearly three-quarters of the adult American population (73%)

[1] The English translation is European Organization for Nuclear Research (CERN, 2007).

routinely accessed the Internet (Madden, 2006, p. 1). When youths and teens are included, approximately 90% of the population accesses the internet on any given day.

Examining the Effects of the Internet on American Society

Over the course of its development, scholars speculated about the impact the Internet would have on society (Tyler, 2002). Some scholars predicted the internet would revolutionize society by changing the basic patterns of social interaction (Tyler, 2002). Other scholars predicted the effects of the internet would be much more conservative (Tyler, 2002). These scholars predicted the internet would merely be a new way of engaging in traditional patterns of behavior (Tyler, 2002).

Despite early speculation about the likely impact the Internet would have on society, only recently have scholars begun to empirically assess the *actual* impact of the internet on society (Tyler, 2002). While a full review of the literature assessing the social impact of the Internet is beyond the scope of this dissertation, the following is a brief description of the types of studies conducted to assess the impact of the Internet on society. Researchers have examined the impact of the Internet on interactions occurring in a commercial setting. Studies have been conducted to assess the impact of the internet on consumer behavior (Fox, 2005), and the effects of conducting business negotiations via an online medium (e.g. electronic mail) (Thompson and Nadler, 2002). Other studies examined the effects of the internet on the leisure activities and pursuit of hobbies by internet users (Madden, 2006), how time spent on the internet affects the amount of time spent on non-internet related daily activities (Nie and Hillygus, 2002). A third group of studies examined the manner in which the internet has affected the interpersonal relationships of internet users. Researchers have examined the effects of the Internet on relationship formation (McKenna, Green and Gleason, 2002), the stability of internet-based relationships relative to

offline relationships (McKenna, Green and Gleason, 2002), the use of the Internet as a forum for establishing an offline dating relationship (Rainie and Madden, 2006), the role of the Internet in helping users cope with the traumatic events, such as the terrorist attacks in 2001, in which the World Trade Center was destroyed (Rainie, 2001), the role of the internet in guiding major life decisions (Horrigan and Rainie, 2006), and the use of internet by stigmatized persons to overcome limitations (e.g. shyness, anxiety, physical appearance and speech impediments) to offline interactions (McKenna and Bargh, 1999, cited in McKenna, Green and Gleason, 2002, p. 9). While efforts to determine the impact of the internet on society, of which the above studies are only a small sample, are still ongoing, it appears that the consensus developing among internet scholars is that the development of the Internet has indeed influenced many aspects of society (Tyler, 2002).

In addition to speculation about the effects the internet would have on conventional aspects of society, there has been a great deal of speculation about the likely effects of the internet on less conventional aspects of society. One such aspect of society is crime. The predicted effects of the internet on crime fall into two general categories: predicted changes in the rates of crime and predicted changes in the nature of crime.

It was predicted that continued development of computers and related forms of technology (e.g. the internet) would change the rates at which various crimes occur. For example, in the late 1970's, August Bequai observed that computer crime had become a growing problem in America (1978). He concluded that the increase in computer crimes was due to two advantages of such crimes over traditional forms of crime. Computer crimes offered greater profits than traditional forms of crime (Bequai, 1978). Offenders committing computer crimes routinely netted profits in excess of twenty times that of offenders committing traditional forms

of crime (Bequai, 1978). In the late 1970's, the average bank robbery netted the offender approximately $15,000, while the average computer crime brought in over $400,000 (Bequai, 1978, p. 105). In addition to larger monetary rewards, computer crimes offered a reduced risk of apprehension and prosecution compared to the risk associated with traditional forms of crime (Bequai, 1978). The odds of a computer crime even being discovered were greatly reduced—with only 1% of computer crimes being discovered (Bequai, 1978, p. 105). Even if a computer crime was discovered, the risk of prosecution was much lower than for traditional offenses (Bequai, 1978). Bequai (1978) predicted increases in the number of computer crimes occurring as offenders realized the advantages of technological forms of crime. Based on his observation, Bequai (1978) predicted that with technological advances in the field of computers "traditional crime may become a thing of the past" (p. 106).

Other scholars predicted the internet would indirectly affect the rates of crime by first changing the opportunities for committing crime. One way in which scholars predicted advances in technology, such as the internet, would change the opportunities for crime was through facilitating and accelerating the shift of America towards a cashless economy (Bennett, 1987; Walker, 1997).

Whereas commercial transactions in pre-World War II *Smokestack America* relied on exchanges of paper forms of cash (e.g. currency, checks and money orders), scholars speculated that the cashless economy of *New America* would rely on electronic fund transfers (e.g. wire transfers and debit or credit card transfers) (Toffler and Toffler, 1990, p. 2). The development of the internet as a venue for commerce accelerated this shift by creating an environment in which buyers and sellers could conduct commercial transactions, without regards to geographic distance, via electronically transferred funds. In other words, the commercial economy that has

developed within cyberspace represents the first example of a cashless economy.

It was predicted that as cashless transactions replace paper-based transactions, the opportunities to commit non-traditional crime would increase and the opportunities for traditional crime would decrease. To compensate for these changing opportunities for committing crime, offenders would either create new forms of crime or adapt traditional forms of crime to be compatible with the electronic means of conducting commercial transactions, resulting in decreases in traditional forms of crime (e.g. theft and forgery of paper checks) and increases in the number of electronic crimes (e.g. theft and uttering of debit and credit cards) (Bennett, 1987; Toffler and Toffler, 1990; Walker 1997). Walker (1997) went so far as to predict that crimes against electronic funds may one day be "the number one crime throughout the world" (p. 274).

Other scholars predicted the internet would change the nature of crime. First, it was predicted that the characteristics of offenders would likely change (Walker, 1997). For example, Walker (1997) predicted that as offenders switch from traditional forms of crime to electronic forms of crime, the proportion of offenders who are white-collar would most certainly increase because white collar workers would be most likely to have the skills needed to commit such crimes. In particular, Walker (1997) predicted a growing portion of offenders would be computer literate. Franklin (2006) suggested that growing numbers of computer literate offenders would be a logical product of the technological revolution and the societal push for parents to raise "computer savvy" children (Franklin, 2006, p. 15). A push to create more computer savvy children now would translate into a greater number of computer savvy offenders in the future (Franklin, 2006).

Finally, scholars predicted changes in the characteristics of those persons with the highest

risk of being victimized. According to these predictions, the group most likely to be crime victims would no longer be those persons between the ages of 18 and 24 years (Bennett, 1987). Within a cashless economy, such as the cyberspace economy, the group most likely to be victimized by crime would be those persons between the ages of 25 and 29 years (Bennett, 1987). Bennett (1987) attributed this increased risk of victimization to two factors. First, the routine activities of 25 to 29 year olds contribute to rising risks of victimization for those within this age group (Bennett, 1987). For example, this segment of the population would be the age group conducting the most cashless transactions and thus would represent the greatest proportion of victims in cyberspace (Bennett, 1987). Second, demographic trends suggest that the size of birth cohorts will continue to grow through the year 2010, resulting in a large portion of potential victims who fall into this age group, which again increases their odds of being a victim of crime in the cashless economy of cyberspace (Bennett, 1987).

Theoretical works by more modern internet crime scholars, writing with the benefit of hind-sight, are generally supportive of the above predictions. The consensus among modern internet crime scholars is that the development of the internet has indeed changed crime in three general ways: by creating new opportunities for crime, by facilitating the commission of traditional forms of crime, and by creating entirely new forms of crime (Wall, 2001).

Routine Activities Theory has been applied to cyber-crime as a means of explaining how the internet has created new opportunities for committing crime (Grabosky, 2001). According to Routine Activities Theory, a crime occurs because three necessary conditions have been satisfied. In order for a crime to occur, motivated offenders must converge, in time and space, with suitable targets without the presence of capable guardians (Felson, 2002; Grabosky, 2001). The internet creates new opportunities for crime by facilitating the convergence of these three

necessary conditions for crime to occur. The internet has created a larger pool of accessible suitable targets, empowered new offenders and reduced the capability of guardians to intervene on the behalf of the victim (Wall, 2001; Pease, 2001). The internet has increased the pool of potential targets. Approximately three-fourths of the American population has access to the internet (Madden, 2006, p. 1). An even larger proportion of American children, teenagers and young adults access the internet (Fox, 2006). In cyberspace, offenders have the potential to interact with millions of other internet users from all parts of the world--each of which represents a possible victim (Wall, 2001). One of the side-effects of the internet, particularly the subsequent development of the World Wide Web, has been to "empower" new offenders who did not have the necessary skills to commit computer crime or traditional forms of crime prior (Pease, 2001, p. 22). The ease of use of the internet and the World Wide Web made it possible for lay-persons to go online, interact with other users in cyberspace, and even engage in criminal behaviors while online (Pease, 2001; Wall, 2001). The addition of newly empowered offenders increased the potential for crime to occur by increasing the number of motivated offenders operating in cyberspace (Wall, 2001). The internet allows motivated offenders access to a "transnational environment" in which time and space are virtually meaningless. In contrast to traditional forms of crime, offenders in cyber-crime may be physically separated from their victims by thousands of miles creating difficulties in investigating and prosecuting internet crimes (Wall, 2001, p. 3). Within the realm of cyberspace, offenders remain largely anonymous making it difficult or, in some cases, virtually impossible to discover the true identities of offenders operating within the virtual environment of cyberspace (Capeller, 2001; Chawki, 2006). Together, the transnational nature and anonymity of cyberspace have significantly decreased the ability for guardians to hold offenders accountable for their illegal actions. In

terms of Routine Activities Theory, the internet has created new opportunities for crime. It has increased the opportunities for crime by increasing the pool of offenders, motivated offenders and by creating an environment in which offenders are less likely to be held accountable for their actions. By facilitating the convergence of the three conditions necessary for crime to occur, the internet has created new opportunities for crime.

Second, the internet has facilitated existing forms of crime (Wall, 2001). The internet facilitates the commission of a wide range of traditional forms of crime, such as murder, child pornography, the sale of illicit goods and services and even domestic violence (Ferraro and Hammer, 2006; Grabosky, 2001). The potential of the internet to facilitate the commission of traditional forms of crime is virtually unlimited. The internet can facilitate the crime by simplifying the mechanical or logistical aspects of the crime, such as facilitating the selection of potential victims or providing a medium for initiating contact with victims, by providing a means of communication for consumers and suppliers in the sales of illicit goods and services (Ferraro and Hammer, 2006, p. 615; Wolak, Finkelhor and Mitchell, 2004; Wall, 2001; Goodman, 2001).

The internet facilitates the commission of traditional forms of crime by reducing both the financial and legal costs of committing such crimes (Ferraro and Hammer, 2006). For example, consider child pornography which has long been criminalized in America (Ferraro and Hammer, 2006). The development of the internet resulted in the ability to purchase materials featuring acts of child pornography at lower costs (Ferraro and Hammer, 2006). Ferraro and Hammer (2006) provide estimates that prior to the development of the internet, a magazine-type publication featuring images of child pornography would have cost $108 (Ferraro and Hammer, 2006, p. 618). The same product purchased over the internet would sell for $25 (Ferraro and Hammer, 2006, p. 618). Similarly, a video depicting various acts of child pornography that sold

for $215 prior to the internet would sell for $50 via the internet (Ferraro and Hammer, 2006, p. 618). Ferraro and Hammer (2006) attributed this reduction in purchase price to the ability to distribute digital media via the internet which made it easier and cheaper to produce and distribute child pornography (Ferraro and Hammer, 2006, p. 618-619). The development of the internet reduced the risk of apprehension and prosecution for those involved in the child pornography industry, both consumers and producers/distributors, by increasing the difficulty of policing child pornography sales and by complicating investigations and prosecutions, and offering a degree of insulation between consumers of child pornography and legal authorities (Ferraro and Hammer, 2006, p. 618).

Finally, the internet has led to the development of entirely new forms of crime (Wall, 2001). Some crimes committed in cyberspace have no traditional crime counterpart and therefore represent entirely new forms of criminal behavior (Wall, 2001). For example, spamming, the distribution of unsolicited commercial messages, is an internet crime with no traditional crime counterpart; and, thus can be considered an entirely new form of crime that occurs only in the context of cyberspace. Other forms of internet crime have traditional crime counterparts, but are so different from that counterpart that they constitute an entirely new form of crime. For example, distributing a virus is essentially an act of vandalism. However, because the financial costs and the difficulties associated with repairing the damage from computer viruses are so much greater than with traditional acts of vandalism the cyber-version of the crime represents an entirely new form of crime (Warren and Streeter, 2005).

In summary, the early futurist writers predicted the internet would affect crime by changing the rates of crime and the nature of crimes. These predictions are generally supported by observations of more modern internet crime scholars. For example, the early futurists

predicted that the technological revolution, in which the internet has played an integral role, would result in changing rates of crime would change the characteristics of both victims and offenders and would change the modus operandi by which offenders commit crime by forcing offenders to adapt to changing opportunities for committing crime. Sykes writing during the early 1970's warned against taking predictions such as those above at face value. Sykes (1970) warns that while "there *is* a certain faddishness in the rush to prophecy[2]", it is important to consider the basis upon which forecasts are created (p. 1). In the case of prophesizing about future of crime, Sykes (1970) warns that "social sciences can scarcely provide an accurate picture of the present (p. 1). However, all things considered, the developing consensus among internet crime scholars is that the internet has affected crime in three ways: it has created new opportunities for crime, facilitated the commission of traditional forms of crime, and even led to the creation of entirely new forms of crime; all three of which are consistent with the above predicted effects of the internet on crime.

Defining Techno-crime, Cyber-crime, Computer Crime and Internet Crime

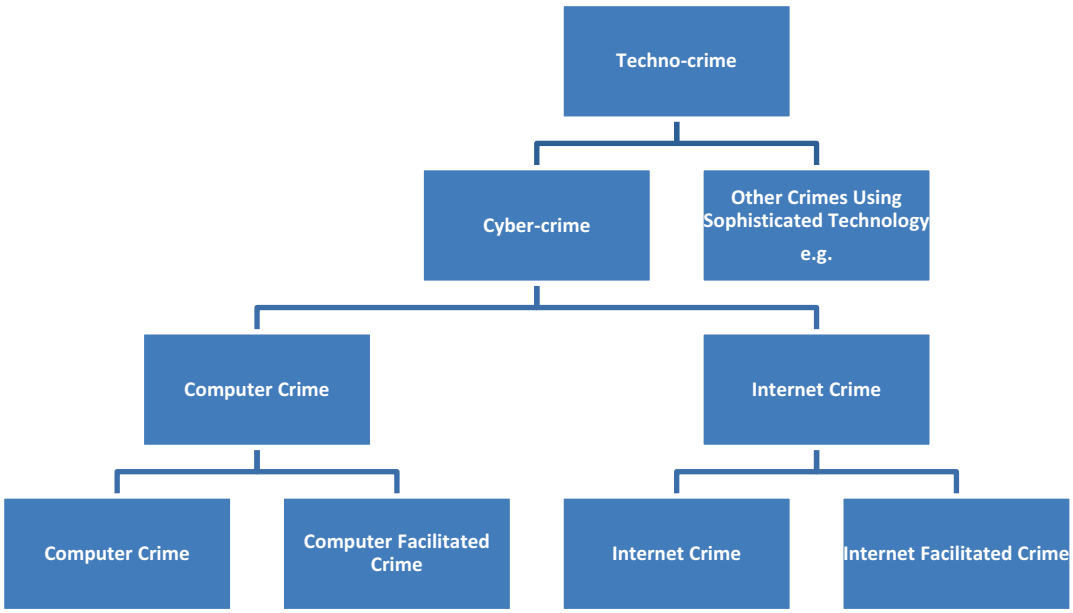
The terms techno-crime, cyber-crime, computer crime and internet crime are used interchangeably, and inappropriately, in the cyber-crime literature (Friedrichs, 2004). As demonstrated in Figure 1.1, these different forms of crime *are* related to one another; however, despite this relationship, these terms are not synonymous. After a careful review of the manner in which these terms are used in the cyber-crime literature, I have crafted definitions for each of these types of crime which demonstrate the relationship between each type of crime, and still maintains the conceptual distinctions of each.

Techno-crime, the broadest of the above forms of crime, refers to *the use of "any*

[2] Emphasis in original.

sophisticated form of technology" to commit an act violating the criminal codes of a specific jurisdiction (Friedrichs, 2004, p. 185). While computers are technologically sophisticated, they are not the *only* sophisticated forms of technology. As demonstrated in Figure 1, each of the other forms of crime is included in the category of techno-crime; however, techno-crime also includes other forms of crime relying on sophisticated forms of technology. For example, war-time atrocities relying on sophisticated forms of technology, or breaking into a vault using sophisticated technology would both be examples of other forms of techno-crime.

Figure 1.1. The Relationship between Techno-crime, Cyber-crime, Computer Crime and Internet Crime.



Cyber-crime is a term which has been used to describe computer crime, internet crime and any other forms of crime in which technological developments are involved. While there have been many attempts to define cyber-crime, many of these definitions have been inadequate. For example, the simplest definitions of cyber-crime would include crimes that are "somehow related to a computer"; however, many crimes have been included as cyber-crime that should not have been included (Wall, 2001, p. 2). In 2005, a series of studies conducted by the FBI

included thefts of laptop computers and other forms of mobile technology under the category of computer crime. These crimes are not cyber-crime (Friedrichs, 2004; Goodman, 2001). These are traditional crimes in which technology was the intended target and serves only an incidental role in the commission of the crime (Friedrichs, 2004; Goodman, 2001). For the purposes of this dissertation, cyber-crime refers to *the use of a programmable, electronic device, either separate from or in conjunction with the internet, to commit or facilitate the commission of an act violating the criminal statutes of a given jurisdiction.* This definition includes two other forms of crime relying on the use of sophisticated forms of technology: computer crime and internet crime.

The term "computer crime" is actually a misnomer (Franklin, 2006). Today, there are many devices, which are not generally considered computers, capable of performing the same actions as a computer (Franklin, 2006). For example, personal digital assistants (e.g. palm pilots and pocket-PC devices) and some cellular telephones are capable of performing many of the same functions as those devices we typically refer to as computers, including accessing the internet. Despite the misnomer that the term computer crime represents, in order to maintain consistency with the existing literature, I have chosen to retain this term to refer to crimes committed by traditional computers, but it is important to note that this definition also includes crimes committed via more modern computer-like devices.

For the purposes of this dissertation, computer crime refers to the *use of a computer or other programmable, electronic device to commit or facilitate the commission of an act violating the criminal statutes of a given jurisdiction.* This definition includes two sub-divisions of crimes committed via computers and computer-like devices: computer crimes and computer facilitated crimes. Computer crimes are those crimes in which an offender uses a computer or other

programmable, electronic device to commit an act violating the criminal statutes of a given jurisdiction. Computer facilitated crime includes those computer crimes in which an offender uses a computer or other programmable, electronic device to facilitate the commission of a traditional crime violating the criminal statutes of a given jurisdiction. Together these two sub-divisions of crime comprise the category of crime better known as computer crime.

Internet crime, a second type of cyber-crime, refers to the *use of a computer or other programmable, electronic device connected to the internet to either commit or facilitate the commission of an act violating the criminal statutes of a given jurisdiction.* As with computer crime, internet crime includes two sub-divisions of crime: internet crime and internet-facilitated crime. Internet crimes are those crimes in which a computer or other programmable, electronic device connected to the internet is used to commit an act violating the criminal statutes of a given jurisdiction. Internet-facilitated crime are those crimes in which offenders rely on the use of a computer or other programmable, electronic device connected to the internet to facilitate the commission of an act violating the criminal statutes of a given jurisdiction.

In summary, while the terms techno-crime, cyber-crime, computer crime and internet crime are used interchangeably, these terms refer to several forms of crime which are fundamentally different from one another, yet related to one another. Furthermore, two of these forms of crime (computer crime and internet crime) include sub-divisions of crime, as well. The categories internet and computer crimes are comprised of new forms of crime which rely on the internet and/or computers and traditional forms of crime facilitated by either the internet or computers. Together, computer and internet crime comprise the category of crimes known as cyber-crime. Cyber-crime and other crimes relying on the use of sophisticated forms of technology comprise the broadest of the above types of crime—techno-crimes.

Examining the Theoretical Framework of the Futurist Writers

As discussed earlier in this chapter, several scholars have made predictions concerning the effect that the ongoing technological revolution and the changing nature of crime—including facilitation of traditional crimes, the adaptation of traditional crimes to fit the information age and the development of completely new forms of crime—will have on the nature of policing in America. While this issue is interesting enough, in and of itself, to merit it becoming the subject of academic research efforts, these predictions of the futurist writers contribute to a larger debate that has been going on for quite some time—the question of how to maximize organizational performance and efficiency.

Organizational theorists have long struggled with the issue of organizational structure[3] and its relationship with maximization of performance and/or efficiency; and, whether environmental demands exert any influence on this relationship. The early scholars, the Classical theorists, focused on the "anatomy of the organization" and developed ways of not only managing, but also designing organizations from their very foundations, with an eye towards enhancing efficiency (Roberg, 1979, p. 24). Classical theorists constructed deterministic organizational theories, which argued that any given organization can only achieve optimum levels of performance if it is designed around *the* proper organizational design (Roberg, 1979). This *proper* organizational design was seen as universally applicable to all organizations, regardless of the environment(s) in which the organization operated. Furthermore, it was argued by the Classical theorists, that organizations must be designed around the proper organizational

[3] Donaldson (1999) defines organizational structure as the "recurrent set of relationships between organizational members" (p. 51). These relationships include authority relationships, reporting relationships (such as would be included on an organizational chart of an organization), as well as organizationally required patterns of behavior, decision-making patterns and communication patterns (p. 51).

design from the moment the organization's metaphorical cornerstone is laid, for organizational design is largely immutable after its creation. In other words, Classical theorists argued that the structures of organizations, once formed, could not be changed in any way which would alter the "fundamental nature of the organization" (Pennings, 1998, p. 41).

For example, Max Weber one of the more famous of the Classical theorists, argued that to achieve optimal levels of performance, organizations needed to be designed around the bureaucratic model—a model he said was "superior to any other form in precision, in stability, in stringency of its discipline and in its reliability" (Weber, 1920; Roberg, 1979, p. 24). Weber's bureaucracy was an organization divided into a formally ordered, hierarchical structure composed of upper and lower offices, or bureaus. This structure relied on adherence to a very strict chain of command, in which the day-to-day activities of workers in lower offices were supervised by those occupying higher offices[4] (Weber, 1920). As new functions developed, the organization would expand to include other bureaus, each functionally differentiated from one another and having control over a "specified sphere of compentence" within the organization (Roberg, 1979, p. 25). Weber, similar to other Classical theorists, viewed organizations as closed systems, in which environmental contingencies were irrelevant to discussions of organizational performance and effectiveness. The primary determinant of *any* organization's effectiveness was the degree[5] to which the organization's structure incorporated *the* proper organizational design, which for Weber meant the characteristics of a bureaucracy.

Structural Contingency Theories

In the early 1960's, Burns and Stalker examined the performance of two types of

[4] Weber argued that in a fully developed bureaucracy, the relationship between upper and lower offices would also be monocratically ordered, meaning that the activities of each lower office is supervised by only one higher office.
[5] Weber's bureaucratic model was an ideal type of organization, in that no organization would fit his model entirely and thus the model served as an example of how an organization should be structured and managed (Roberg, 1979).

structures in various environments: the mechanistic structure[6] and the organic structure[7] in stable and changing environments (Burns and Stalker, 1961). They found that organizations characterized by a mechanistic structure were more effective in stable environments and organizations incorporating an organic structure were more effective in, and thus better suited to, changing environments (Burns and Stalker, 1961). These findings contributed support to the growing idea that different organizational designs might be more or less effective in different organizational environments and the subsequent development of structural contingency theories of organizational design (Pennings, 1998).

Research into the effects that environments had on the organizations operating in them continued throughout the 1960's; and, by 1970, the Contingency theory approach to studying organizational design and performance was well established (Donaldson, 1996). Today, structural contingency theory is a "major theoretical lens" through which organizational scholars have examined organizations, as well as, their design and performance (Donaldson, 2001, p. 1).

The development of this new approach to understanding organizational design represented a direct challenge to the normative arguments of the classical theorists and views concerning the immutability of organizations. Whereas the classical theorists argued that organizational effectiveness depended on conformity with a universally effective organizational design, structural contingency theories argue that enhanced organizational performance requires organizations to adopt "some rational calculus in optimizing the organization to its

[6] Mechanistic structures are characterized by a high degree of structure and are more bureaucratic in their designs (Roberg, 1979). Mechanistic structures produce the highest levels of organizational performance when coupled with employees who are relatively inexperienced and/or unskilled who have a strong need for security and stability; and who operate in a relatively stable environment performing programmable tasks with standardized materials.

[7] Organic structures are characterized by a low degree of structure of and are non-bureaucratic in their designs (Roberg, 1979). They produce the highest levels of effectiveness when paired with highly skilled employees who are widely distributed; with employees who have a high level of self-esteem and a strong need for achievement, autonomy and self-actualization; and an operational environment characterized by rapidly changing technology and non-routinized and non-programmable tasks.

environmental conditions" (Pennings, 1998, p. 40). In other words, structural contingency theories were not a universalistic theory arguing that optimally performing organizations should be based on some single optimal design, but rather that the proper organizational design will be contingent on the various environmental influences, or contingency factors, in the organizational environment (Donaldson, 1985).

Organizations can encounter any number of possible contingency factors, as a contingency factor can be "any variable that moderates the effect of an organizational characteristic on organizational performance" (Donaldson, 2001, p. 6). Some of the more common contingency factors discussed in the academic literature include: the strategy of the organization, the organization's size, the degree of uncertainty in the organization's environment, the complexity of the organization's consumer base, as well as the available and developing forms of technology (Donaldson, 1999; Pennings, 1998).

While the structural contingency approach argues against the universal effectiveness of an organizational design and acknowledges the necessity of tailoring an organization's design to fit its environment, it would be unfair to characterize structural contingency theories as eschewing any guiding principles of organizational design. Contingency theories attempt to establish "a middle ground between 'universalistic principles' and 'it all depends'" (Roberg, 79, p.74). In its most basic form, "the contingency approach considers [the] specific organizational circumstances and attempts to apply the most appropriate organizational designs and managerial practices to particular situations" (Roberg, 1979, p. 15).

The predictions of the futurist authors, discussed earlier in this chapter, that the technological revolution and the development of a cashless society will change the nature of crime and by extension, the nature of policing, are consistent with the basic tenets of the

structural contingency theory framework. In essence, the futurist writers in predicting social change were also predicting changes to the environmental contingency factors that would influence law enforcement agencies in America.

This section has discussed the theoretical framework of structural contingency theories. Structural contingency theories argue that the proper organizational design is one which conforms to various environmental conditions (i.e. contingency factors) that a specific organization encounters. This non-universalistic, non-deterministic and non-normative theory or organizational design was a direct challenge to theories that asserted that the adoption of a universally applicable "best" organizational structure was the key determinant of organizational design.

Statement of the Problem

If the futurist authors were correct and the technological revolution, of which the internet has played no small part, has changed the nature and rates of crime in America, it is plausible that such changes could also affect the role of local law enforcement agencies in controlling internet crime. In fact, some of the futurists predicted that changes in crime would indeed affect local law enforcement agencies. For example, Walker (1997) predicted that the changing characteristics of offenders would also change the characteristics of police officers, such as officers becoming more technologically proficient, and create a new breed of police officer. Toffler and Toffler (1995) predicted changes associated with the technological revolution would result in the last decade of the 20th century being one of the most challenging eras for law enforcement officials.

Despite the plausibility of such claims, there have been few efforts to empirically examine how the development of the internet and internet crime have *actually* changed the

manner in which local law enforcement agencies address crimes when those crimes either occur or are committed in cyberspace. This observation is consistent with a general trend in the sociology of technology that began at about the same time as the technological revolution (Fischer, 1985). Beginning in the 1950's, there was a decline in the number of empirical studies appearing in scholarly journals which examined the effects of technology on society (Fischer, 1985). Ironically, while the number of empirical studies examining the effects of technology on society declined, there was no corresponding decline in the number of empirical studies examining how society influences the development of technology (Fischer, 1985). While it appears that this trend has been reversed in regards to more conventional aspects of society, there is little evidence to suggest that this trend has been reversed in terms of the effects of technology on crime and on the role of those seeking to control such forms of crime.

The failure to empirically examine the effects of technological advances, such as the internet, on the role of local law enforcement agencies in controlling crime represents a significant oversight in the policing literature. As a result of this oversight, much of our understanding about the role local law enforcement agencies in the latter half of the 20th century serve in controlling internet crime is based on anecdotal evidence, such as news stories highlighting the actions of a single police department. Also, as a result of this oversight, scholars are unable to articulate the current role law enforcement agencies serve in controlling crime. In lieu of data about the role of local law enforcement agencies in controlling internet crime, scholars have generalized our understanding of their role in controlling traditional forms of crime to the role in controlling internet crime. This generalization contributes to assumptions that police are actively involved in controlling internet crime. For example, a recent textbook, written for corporate investigators of cyber-crimes, advises investigators to contact local law

enforcement if they have any problems stating that "local authorities will, if they have the resources, usually be glad to get involved" (Stephenson, 2000, p. 13). Statements such as this seem inappropriate, or at least premature, in that we know neither the willingness of local law enforcement agencies to get involved in internet crime investigations nor the frequency with which they receive internet crime complaints. Furthermore, we do not know the activities in which local law enforcement agencies engage in controlling various forms of internet crime.

In summary, little is known about the current role of local law enforcement agencies in controlling crime. Little is known about the preferred and the enacted roles of such agencies in controlling internet crime. Beyond, filling a void in the academic understanding of local police agencies, if scholars such as Heaphy (1978), who states that police improvement depends on agreement between police priorities and citizen demands, and Barlow and Barlow (1999) and Lyman (2002) are correct in their assertion that the legitimacy of police agencies originate in them being accountable to the community, these issues may be affecting the legitimacy of local law enforcement agencies. Only through research into the extent to which internet crimes occur and the extent to which the community calls upon local law enforcement agencies to control such crimes can we understand how this issue affects the legitimacy of such agencies. In short, it is essential that policing scholars begin to correct the above oversight in the policing literature.

The Current Study

This dissertation begins the process of rectifying the above oversight in the policing literature by empirically examining how the effect of the internet on crime may have affected the nature of the role of police in controlling internet crime, and an examination of the variables explaining any observed variation. The data upon which this study is founded were collected via a survey questionnaire mailed to the chief administrators of a sample of local law enforcement

agencies, including both municipal police departments and sheriff departments[8], in the state of Ohio.

The first step taken towards rectifying this oversight is to articulate the current role local law enforcement agencies serve in controlling internet crime in terms of the three dimensions of the role of local law enforcement agencies in controlling crime (Burton et al., 1993). The first dimension of the crime control role is the prescribed role (Burton et al., 1993). This role is defined in legal statutes of a given jurisdiction which authorize the police to intervene in crime occurrences. This dimension of the crime control role dictates what the police should be doing to control crime (Burton et al., 1993). The second dimension of the crime control role of law enforcement agencies, the preferred role, represents what the community and police officers within a department would like the role of the police in controlling crime to be (Burton et al., 1993). This dimension can be observed via the calls for service an agency receives from the community, and via the preferences of law enforcement officers within a specific agency. The current study only examines the community assigned, preferred role of law enforcement in controlling internet crime. No attempt is made to determine the crime control role local law enforcement officers would prefer. The final dimension of the role of the local law enforcement agencies in controlling internet crime, the actual role, represents the actual activities of law enforcement agencies in controlling internet crime (Burton et al., 1993). The actual role a law enforcement agency serves in controlling crime is the product of a negotiation process in which each agency assigns different priorities to both the prescribed and preferred crime control roles assigned to it (Burton et al., 1993). The three dimensions of the crime control role exist

[8] As will be discussed in greater detail in Chapter Four, county sheriff's departments are to be included in the current sample, because in many rural areas of Ohio, county sheriff departments serve the same primary law enforcement functions as municipal police departments in incorporated areas.

simultaneously within each law enforcement agency; however, the degree to which these dimensions align can vary across different departments, or even between various groups (such as the patrol division and investigative division) within a law enforcement agency.

In articulating the actual role of law enforcement agencies in controlling internet crime, the present study examines a wide range of possible responses by local law enforcement agencies, such as engaging in reactive investigations, proactive investigations, distributing preventative literature, arresting offenders, referring complainants to another agency, creating a specialized division to investigate internet crime complaints, and/or joining an internet crime task force. In examining the preferred role of law enforcement agencies in controlling internet crime, prior studies have focused on a relatively limited range of internet crimes. The current study will examine the volume of internet related calls for service received by law enforcement agencies in the sample including a very wide range of internet-related crimes. The full range of internet crimes included in the current study is discussed in Chapter Four. Finally, while not empirically examined in this study, the prescribed role of law enforcement agencies in controlling internet crime, represented by the statutes in the criminal law which govern the intervention of local law enforcement agencies in internet crime complaints, is held constant[9]. Since the sample includes only local law enforcement agencies in Ohio, it is assumed that the prescribed role of the various law enforcement agencies included in the sample is identical across such agencies. This feature of the current study will be discussed in greater detail in Chapter Four of this dissertation.

In summary, in the current study, a mail survey was distributed to the chief administrators

[9] The author concedes that the prescribed role is not totally controlled for, because while the variation due to the state level criminal law is held constant, there is the possibility for variation in local ordinances and agency regulations.

of a sample of local law enforcement agencies in Ohio in an effort correct a significant oversight in the policing literature and articulate the current role of local law enforcement agencies in controlling internet crime. This role is conceptualized as being multi-dimensional. The three dimensions of the role of local law enforcement agencies in controlling internet crime are the prescribed role, the preferred role and the enacted role. In addition to articulating the current role of local law enforcement agencies, the current study will also identify the major correlates of variation in the role local law enforcement agencies serve in controlling a wide range of internet crimes in the state of Ohio.

Summary/Concluding Remarks

Since just after the close of World War II, modern American society has been in the midst of a technological revolution. This technological revolution has transforming American society into an "information society" in which the accumulation of skills, information and knowledge are valued commodities. This revolution has also bombarded Americans with a flood of technological advances and innovations which further the pursuit of information production and use within a wide array of different fields. One such technological advance has been the development of the internet.

Despite a great deal of speculation as to the effects the internet would have on society, until recently there has been very few empirical studies examining the actual effects of the internet on society. Since the turn of the 21st century there has been a revival in the empirically examining the societal effects of the internet; however, there continues to be little scholarly attention devoted to assessing the effects of the internet on crime and the role of local law enforcement agencies in controlling internet crime.

The current study is an effort to rectify this oversight in the policing literature by

empirically examining and articulating the current role of local law enforcement agencies in controlling internet crime. The crime control role served by local law enforcement agencies is conceptualized as being composed of three different dimensions. The prescribed role represents the role that law enforcement agencies are supposed to serve, while the preferred role represents the role that the community and police officers would like law enforcement agencies to serve. Finally, the enacted role reflects the role that law enforcement agencies actually serve in controlling internet crime. The current study articulates the current role of local law enforcement agencies in controlling internet crime in terms of each of these dimensions and examines the degree to which these various dimensions are aligned, or misaligned, with one another.

Chapter Two of this dissertation reviews the existing empirical literature measuring the extent to which various forms of internet crime occur in America. While this literature is quite limited, it is possible to gain at least a preliminary indication of the amount of internet crime occurring in America, and the relative prevalence of various forms of internet crime. Chapter Three reviews the existing theoretical and empirical literature of police organizations and organizational change. Chapter Four discusses the methodology of the current study and describes how the variables were operationalized. Chapter Five discusses the analysis of the data and the specific findings of the present research. Finally, Chapter Six presents the conclusions and summaries of the current study.

Chapter Two: Literature Review

Internet Crime

The current chapter reviews the cyber-crime literature addressing two issues of critical importance to the present study. The first section of this literature review presents findings from various empirical studies assessing the prevalence of internet crimes in America. This portion of the literature review is intended to acquaint the reader with the most commonly occurring types of internet crime. The second section of this chapter reviews the literature examining the proportion and types of internet crime victims report to law enforcement agencies.

Two Types of Internet Crimes

Many schemes exist for classifying internet crimes into discreet groups based on various characteristics of internet crimes (e.g. Wall, 2001; Grabosky, 2005; Goodman, 2001; Carter, 2001; Hammer and Ferraro, 2006). However, a review of the theoretical internet-crime literature concerning the effects of the internet on crime suggests that, at the most basic level, there are different types of internet crime. In Chapter One I discussed the three effects the internet has had on crime. The following section briefly reviews these effects and presents a parsimonious classification of internet crime which provides a framework for the remainder of this chapter.

There is a general consensus among internet crime scholars that the internet has had three effects on the nature of crime. First, the internet has created new opportunities for committing existing forms of crime (Wall, 2001; Goodman, 2001). Second, the internet has facilitated the commission of traditional forms of crime (Wall, 2001; Goodman, 2001). Finally, the internet has led to the creation of entirely new forms of crime (Wall, 2001; Goodman, 2001).

Based on the above effects of the internet, it appears that at the most basic level there are two types of internet crime. The first type of internet crime—which I refer to as *internet-related*

traditional crime—includes all forms of internet crime in which offenders rely on the use of the internet, to either facilitate or commit a traditional form of crime[10]. The second form of internet crime—referred to hereafter as *internet crime*—includes those crimes in which offenders rely on the use of the internet to commit the offense, and for which there is either no traditional crime counterpart or is significantly different from a corresponding traditional crime, and thus constitute an entirely new form of crime. In reviewing the existing literature examining the prevalence of various forms of internet crime, the following section is organized in terms of these two types of internet crime.

Prevalence of Internet-Related Crime

Internet-related traditional crimes are those crimes in which the offender relies on the use of the internet to facilitate or commit a traditional crime. These crimes are virtually indistinguishable from traditional forms of crime, except that offenders of these crimes depend on the internet to either facilitate or commit the offenses.

Internet-related Fraud

Studies of internet crime have found that internet-related fraud[11] comprises a large portion of the internet-related criminal victimization in America. For example, the Internet Crime Complaint Center (IC3) found that a large proportion of the 200,481 complaints received during the 2006 calendar year were internet-related frauds. Of the complaints received by the IC3 in 2006, approximately 43%—86,279 complaints—were referred to a federal, state or local policing agency for further investigation. Of the complaints that were referred to various police

[10] Consistent with a distinction made by Goodman (2001), internet-related traditional crime category of internet crime does not include crime in which the use of the internet is merely incidental to the crime. For example, if an offender uses the internet to find the address of a bank for the purposes of armed robbery, this crime would not be classified as an internet-related traditional crime. Such a crime would simply be considered a traditional armed robbery.

[11] Fraud is defined as "the use of misrepresentation or deception to induce someone to hand over money or something else of value (Henderson, 2005, p. 54).

agencies, the majority of complaints concerned internet-related frauds: 44.9% involved internet auction frauds, and another 19% concerned non-delivery of a service and/or product (IC3, 2007, p. 3).

Internet crime studies have found businesses to be likely targets of fraud. For example, two studies of cybercrimes conducted by the FBI in 2005 indicate that approximately 9% of businesses detecting an incident of cyber-crime had been victims of financial fraud, and 5-8% of such businesses were victims of telecommunications fraud (FBI, 2005, p. 6; Gordon et al., 2006). These percentages are higher than those found by Randala (2004). Randala (2004) found that only 2% of businesses, surveyed in 2001, reported being victimized by internet-related forms of fraud[12].

A sub-category of internet-related fraud, internet-related identity theft, has received a great deal of media attention in recent years; however, despite this attention, relatively little has been done to determine the actual extent to which identity theft is committed via the internet. In 2003, the Federal Trade Commission surveyed American households about their experiences with identity theft. Overall, nearly 5% of respondents indicated that they had been the victim of identity theft within the past year. The Federal Trade Commission extrapolated this finding to the population resulting in an estimate that nearly 10 million Americans had been the victim of identity theft in the year previous to the study (FTC, 2003). Of the cases of identity theft reported by survey respondents, approximately 3% involved an offender fraudulently using one or more of the victim's existing internet or email accounts; and, approximately 2% of identity theft cases involved an offender who fraudulently opened new internet or email accounts in the victim's name (FTC, 2003, p. 33, 34). Due to aggregation biases in the data, it is not possible to

[12] The data analyzed by Randala (2004) included fraud and embezzlement in the same category, and included non-internet-based forms of crime, as well.

draw any further conclusions from the FTC data. However, McQuade and Schreck (2004) analyzed data from a survey of college students at Rochester Institute of Technology and found that 6% of respondents had been victims of online identity theft within the previous year (cited in McQuade, 2006, p. 193).

Online Harassment and Cyber-stalking

Online harassment—defined as use of the internet to engage in a pattern of behavior, which may or may not include threats that "persistently" annoy or torment another person—can take many different forms and affect many different types of victims (McQuade, 2006, p. 93). For example, in a study of college students at Rochester Institute of Technology, McQuade and Schreck (2004) found that 17% of respondents had been harassed online within the previous twelve months (cited in McQuade, 2006). Analyses of data from the Youth Internet Safety Survey (YISS) found that 6% of youth between the ages of 10 and 17 years had been victims of online harassment[13] within the previous year (Finkelhor, Mitchell and Wolak, 2005). Analyses of the Second Youth Internet Safety Survey (YISS-2) data indicate that within the five years since the first YISS was conducted, the percentage of youth reporting online harassment rose from 6% to 9%, a statistically significant ($p \leq 0.05$) increase of 50% (Wolak, Mitchell and Finkelhor, 2006, p. 39). The YISS-2 questionnaire included a sub-classification[14] of online harassment—chronic online harassment—which allowed researchers to distinguish between youth experiencing one or two isolated incidents of harassment and youth experiencing three or more incidents of harassment (Wolak, Mitchell and Finkelhor). An analysis of the YISS-2 data found that while relatively few of the youth in the sample were victims of online harassment

[13] In both the original and the second Youth Internet Safety Survey, online harassment was operationalized as "threats or other offensive behavior (not sexual solicitation), sent online to the youth or posted online about the youth for others to see" (Wolak, Mitchell and Finkelhor, 2006, p. 3).

[14] This distinction was not made in the original YISS and therefore no comparisons can be made between the findings of the two surveys in regards to online harassment of youths.

during the previous year, approximately 32% of those who did experience online harassment were victims of chronic online harassment[15] (Ybarra et al., 2006, p. e1169).

Cyber-stalking, which has received a great deal of media attention in recent years, represents an extreme form of online harassment. It is difficult to obtain accurate estimates of the number of cyber-stalking incidents that occur because like traditional stalking, cyber-stalking is not so much a criminal act as it is a series of acts (e.g. pursuit behaviors[16]) which together constitute a crime (Henderson, 2005; NIJ, 1999). Furthermore, the task of obtaining an accurate estimate of the number of cyber-stalking incidents occurring is hindered by the lack of an agreed upon definition of cyber-stalking, which makes it difficult to determine where exactly online harassment ends and cyber-stalking begins (Henderson, 2005; NIJ, 1999). While scholars have not agreed upon a definition of cyber-stalking, the following definition of cyber-stalking is representative of a *typical* definition of cyber-stalking (NIJ, 1999; Henderson, 2005). Bryan (2001) defines cyber-stalking as "the act of threatening, harassing or annoying someone through multiple email messages or through the internet, especially with the intent of placing the recipient in fear that an illegal act or an injury will be inflicted on the recipient or a member of the recipient's family or household" (cited in Henderson, 2005, p. 35). Other variations of this definition limit the person against whom any threats must be made. Some require the threats be made against the primary victim, while other definitions, such as the one above, incorporate threats against anyone (Henderson, 2005). Definitions such as that used by Fisher, Cullen and Turner (2002) in studying stalking behavior, in general, define stalking as "obsessive behavior" (p. 261).

[15] In terms of the Second Youth Internet Safety Survey, chronic online harassment was operationalized as three or more incidents of online harassment within the past year (Ybarra et al., 2006, p. e1169).
[16] Consistent with the work of Fisher, Cullen and Turner (2002), the term "pursuit behaviors" is used to distinguish between the individual acts that comprise a cyber-stalking incident and the full incident of cyber-stalking.

There have been relatively few attempts to quantitatively study the cyber-stalking phenomenon. However, there is evidence to suggest that incidents of cyber-stalking are a growing challenge for law enforcement agencies nationwide (NIJ, 1999). Unfortunately, a great deal of the evidence comes from studies of traditional stalking incidents. For example, a 1999 report from the Attorney General of the United States, which generalized the findings of the National Violence against Women survey concerning stalking to the more specific category of cyber-stalking, concluded that well over 100,000 Americans might be recent victims of cyber-stalking (NIJ, 1999).

Empirical studies of internet-crime, which include cyber-stalking, tend to find a smaller number of incidents of cyber-stalking than the above estimate from the Attorney General's report to Vice President Al Gore. Many of these empirical studies have relied on surveys of college students. For example, an analysis of the data collected in a study of college students at Rochester Institute of Technology, McQuade and Schreck (2004) found that 6% of respondents were victims of cyber-stalking within the previous year (cited in McQuade, 2006, p. 193). Findings from a national-level survey of female college students, conducted by scholars at the University of Cincinnati during the 1996-1997 academic year, found that of 4,446 survey respondents, approximately 13% had been stalked in some manner at least once. Of the 696 stalking incidents reported by 581 stalking victims, 24.7% of the "pursuit behaviors[17]" included contacts via email, and therefore constitute incidents of cyber-stalking (NIJ, 1999; Fisher, Cullen and Turner, 2002, p. 282).

In addition to studies of cyber-stalking focusing on college students, the national safety organization Working to Halt Online Abuse (WHO@) (sic), compiles statistics of the

[17] The authors used the term "pursuit behavior" to distinguish between individual acts committed that together constitute an "incident" of stalking (i.e. a series of actions) (Fisher, Cullen and Turner, 2002, p. 282).

characteristics of cyber-stalking complaints received from victims each year. These statistics indicate that between 2000 and 2006, WHO@ received a total of 2036 complaints of cyber-stalking incidents from victims (WHO@, 2007). Of these cases, the vast majority of victims were female, and the vast majority of offenders were male. However, victims were equally likely to be stalked online by someone they know as to be victimized by strangers.

Internet-related Sex Crimes against Juveniles

The first and second versions of the Youth Internet Safety Survey, conducted by the Crimes against Children Research Center at University of New Hampshire studied the percentage of youths between the ages of 10 and 17 years were victimized by two different types of internet-related sex crimes: unwanted sexual solicitations of youths and unwanted exposure to online sexual images (Mitchell, Finkelhor and Wolak, 2001; Finkelhor, Mitchell and Wolak, 2005). The following section discusses the findings of the YISS and YISS-2 concerning the prevalence with which these crimes were experienced by youths in each sample.

Approximately 19% of youths surveyed as part of the YISS, in 2000, had received some form of internet-based unwanted sexual solicitation—defined as requests to "engage in sexual activities or sexual talk or to give personal sexual information"—within the previous year (Finkelhor, Mitchell and Wolak, 2005, p. 437; Mitchell, Finkelhor and Wolak, 2001, p. 3012). Online sexual solicitations included requests for the youth to engage in cyber-sex[18] with the solicitor, questions about the measurements of the youth's body (e.g. asking about the youth's bra size), engaging in general discussions about sexual topics, and questions about the youth's sexual experience (e.g. if the youth was a virgin) (Finkelhor, Mitchell and Wolak, 2005, p. 444, 445).

[18] Cyber-sex is "a form of fantasy sex that involves interactive chat room sessions during which the participants describe sexual acts and sometimes disrobe and masturbate" (Finkelhor, Mitchell and Wolak, 2005, p. 444).

Analyses of data from the YISS-2, collected in 2005, found that a smaller proportion of youths in the sample received sexual solicitations within the previous twelve months, than had been found in the YISS data from 2000 (Wolak, Mitchell and Finkelhor, 2006). Whereas 19% of youths in the YISS sample had received sexual solicitations, only 13%[19] of youths in the YISS-2 sample had received such a solicitation, a statistically significant difference ($p \leq 0.05$) (Wolak, Mitchell and Finkelhor, 2006, p. 7). In addition to sexual solicitations of youth, findings from the YISS-2 indicate that a large proportion of online sexual solicitations received by youths were ones in which the solicitor requested a photograph of the youth (56%), and a sizeable minority of online sexual solicitations (27%) were ones in which the solicitor requested a sexually-oriented photograph of the youth (Wolak, Mitchell and Finkelhor, 2006).

In addition to unwanted sexual soliciations, the First and Second Youth Internet Safety Surveys asked youths about aggressive sexual solicitations, which were defined as those online sexual solicitations that also included an attempt by the solicitor to contact the youth via some means other than the internet, such as via the telephone, in person, or through traditional mail) (Finkelhor, Mitchell and Wolak, 2005, p. 440). Data from the YISS and the YISS-2 indicate that less than 5% of the youth in each sample experienced an aggressive sexual solicitation (Finkelhor, Mitchell and Wolak, 2005, p. 440). While the overall prevalence of these solicitations did not change between the YISS and YISS-2, the overall pattern of behaviors did change. For example, aggressive sexual solicitations included requests to meet the solicitor somewhere (66% in YISS, 75% in YISS-2), solicitors sending mailings via traditional mail (39% in YISS, 9% in YISS-2), or sending money and/or gifts to the youth (5% in YISS, 12% in YISS-2), calling the youth on the telephone (14% in YISS, 34% in YISS-2), going to the youth's house

[19] Wolak, Mitchell and Finkelhor (2006) found this decline to be statistically significant (p. 7).

(2% in YISS, 18% in YISS-2), and buying a plane, traffic or bus ticket for the youth to meet with the solicitor (2% in YISS, 3% in YISS-2) (Finkelhor, Mitchell and Wolak, 2005, p. 443). The above findings suggest that while the overall prevalence of aggressive sexual solicitations did not change, the activities involved in such solicitations did—it appears they became more personal. For example, the percentage of solicitations via the postal service declined by 30%, while the percentage of solicitations involving attempts to telephone youths increased by 20% and the percentage of solicitations involving attempts to visit the youth at home increased by 16%.

A second form of internet-related sex crime against youths that was studied by the YISS and YISS-2 were incidents in which youths were exposed to unwanted online sexual images. The vast majority of youths were exposed to images of nudity and sexual acts, however a small proportion of youths were exposed to images depicting acts of sexual violence (Finkelhor, Mitchell and Wolak, 2005, p. 450).

In the YISS, 25% of youths surveyed had been exposed to unwanted sexual images via the internet or email (Finkelhor, Mitchell and Wolak, 2005) By 2005, when the YISS-2 was conducted the percentage of youths exposed to unwanted sexual material had risen to 34%, a statistically significant increase ($p \leq 0.05$) (Wolak, Mitchell and Finkelhor, 2007). This increased exposure of youth to such images was visible in all age groups and in both gender groups, and occurred despite a 22% increase in the percentage of households using software to filter, monitor or block unsuitable content (Wolak, Mitchell and Finkelhor, 2007).

Both the YISS and YISS-2 found that the majority of youths exposed to online sexual images were browsing the web at the time of the incident. The most common means by which youths were exposed to such images occurred when the youth opened a hyper-text link generated by an online search of a non-sexual topic, when the youth misspelled a website address, and

when the youth opened a hyper-text link which appeared on a website the youth was visiting at the time of the incident (Finkelhor, Wolak and Mitchell, 2005). A smaller but substantial portion of the exposures originated from links sent to youths in emails; the majority of which were sent to email accounts that only the youths used (Finkelhor, Wolak and Mitchell, 2005). (Finkelhor, Wolak and Mitchell, 2005).

Internet Crime

As stated at the beginning of this chapter, internet crimes are those crimes in which offenders rely on the internet to either facilitate or commit the offense, which either have no traditional crime counterpart, or are significantly different from traditional forms of crime, that they constitute entirely new forms of crime. The current section discusses a number of these internet crimes including: malware attacks, denial of service attacks, and attempts to gain unauthorized access to a computer, computer system or computer accounts.

Malware Attacks

One of the most consistent findings in the internet-crime literature is the frequency with which businesses report attacks upon their computer systems and/or networks by malicious software (i.e. malware). These attacks are often designated as the most problematic cyber-crime incidents experienced and can involve a number of different types of victimizations (Randala, 2004). For example, a computer virus attack involves the introduction of a self-replicating program which identifies and imbeds itself in executable programs installed on the infected computer. These programs have the potential to destroy data stored on a computer, corrupt or damage hardware or result in other harmful effects (McQuade, 2006, p. 65). Viruses only replicate when an infected file is opened and/or executed; therefore, it is said that the victim of a computer virus cooperates in his or her own victimization by opening the original infected file

(McQuade, 2006). A network worm is a "self-contained program (or set of programs) capable of spreading complete copies or segments of itself to other computers" (McQuade, 2006, p. 65). Unlike computer virus programs, worms can replicate and become active without the victim opening an infected file (McQuade, 2006). For example, visiting an infected website can result in an infection by a network worm (McQuade, 2006). A trojan program is a program which appears to be doing one task while it is actually doing another task which its designer has specified (McQuade, 2006). For example, a spy-ware program, which is a form of a trojan program, will surreptitiously track the activities and behaviors of a computer's user(s) and send the collected information to a remote location, usually to the company distributing the spy-ware program (Molyneux, 2003, p.226).

Studies of cyber-crimes committed against businesses have consistently found large numbers of respondents victimized by malicious software (i.e. malware) attacks. Randala (2004) analyzed the data from a pilot study of cyber-crimes against businesses conducted in 2001 and found that 64% of businesses in the sample had detected a computer virus attack (including viruses, worms and trojan programs) (p. 3). When only those businesses detecting a cyber-crime incident were considered, over 89% of such businesses were victims of computer virus attacks (Randala, 2004, p. 3). The findings from analyses by both the FBI (2005) and Gordon et al. (2006) are consistent with those of Randala (2004). Gordon et al. (2006) found that 65% of businesses surveyed were victimized by at least one computer virus attacks in the past year (p. 13). An analysis by the FBI (2005) found nearly 84% of responding businesses reported being attacked by computer viruses, and 79% reported being victimized by spy-ware programs (FBI, 2005, p. 6).

In addition to businesses being victimized by computer viruses and other forms of

malware, individual users are also the victims of such attacks, however, the evidence is much more limited. In analyzing the data from a study of college students at Rochester Institute of Technology, McQuade and Schreck found that 17% of sample respondents had been victims of computer viruses (cited in McQuade, 2006).

Denial of Service Attacks

A second type of internet crime, which is commonly reported by businesses, is a denial of service attack. Denial of service attacks involve attacks on a computer network, host or server which make it difficult for authorized users to connect to the targeted system (Molyneux, 2003, p. 286). There are many forms of denial of service attacks (Molyneux, 2003). For example, a distributed denial of service attack uses a large number of computers—usually "zombie" computers that have been commandeered by a trojan program—to launch a denial of service attack with all of the affected computers attacking in unison (Molyneux, 2003, p. 133, 286). Other denial of service attacks originate from a single computer and attempt to block legitimate access to a computer network, by clogging the targeted network with a large number of illegitimate requests for service (Molyneux, 2003, p. 133).

While cyber-crime studies of business find a relatively smaller proportion of respondents victimized by denial of service attacks than by malware attacks, the amount of financial loss suffered by the victim of a denial of service attack can be extremely large (Randala, 2004; FBI, 2005; Gordon et al., 2006). For example, analyses by Randala (2004), the FBI (2005), and Gordon et al. (2006) all indicate that between 12% and 25% of businesses reported experiencing at least one denial of service attacks in the past year; however, the estimates of the total costs

associated with denial of service attacks range between almost $3,000,000 and $14,400,000[20] (Randala, 2004; FBI, 2005; Gordon et al., 2006).

Computer Hacking

A third type of internet crime involves gaining, or attempting to gain, unauthorized access to a computer, computer system, or computer accounts of another; a crime more commonly known as computer hacking. The means of computer hacking can range from such unsophisticated methods as guessing another user's password to means requiring highly specialized technical and programming skills; and, computer hacking victims can range from the run-of-the-mill homeowner who uses the family computer for recreation to multinational corporations who routinely transfer millions of dollars via the internet.

In a study of college students in an unnamed southern university, Skinner and Fream (1997) found that approximately 21% of the students surveyed had attempted to guess someone else's password sometime in the past, approximately 16% had attempted to guess a password in the past year, and 5% had done so within the past month (p. 508). In addition to guessing passwords, 17.6% of students reported having actually gained unauthorized access to someone else's computer account or files to browse the contents, at some point in the past, approximately 13% reported having done so in the past year, and 4.8% had done so in the past month (Skinner and Fream, 1997, p. 508). A much smaller proportion of respondents (7.4%) indicated that they had ever gained access to someone else's account without authorization, for the purpose of adding, deleting, changing or printing some part of the content, and 5% admitted to having done

[20] The estimates from an analysis conducted by Randala (2004) yield a significantly higher loss due to denial of service attacks than both the estimates of analyses by the FBI (2005) and Gordon et al. (2006). This difference is partially explained by an overall decrease in the number of reported denial of service attacks from 2001, when the data analyzed by Randala was collected, and 2005, when the data analyzed by Gordon et al. (2006) was collected. Graphic depictions of trends in the percent of respondents experiencing a denial of service attack suggest that between 2000 and 2005, there was an overall decrease of over 10 percentage points (Gordon et al., 2006, p. 13).

so within the past year, and 1.5% of respondents admitted to having gained access to another's accounts or files in order to change or print the content within the past month (Skinner and Fream, 1997, p. 508).

Studies of internet crimes against businesses vary in their estimates of the prevalence of unauthorized access to information (i.e. computer hacking). At least some portion of the difference between the various estimates is likely due to the manner in which computer hacking was operationalized. For example, an analysis by the FBI (2005) suggests that a relatively small proportion of businesses—approximately 4%—reported someone accessing their intellectual property or proprietary information, without authorization, within the past year; however, Gordon et al. (2006) found that within the past year, 32% of surveyed businesses reported incidents in which someone gained access to their digitally stored information. In the FBI (2005) study?data computer hacking of information was limited to incidents in which offenders accessed the company's intellectual property or proprietary information (p. 6). In the data analyzed by Gordon et al. (2006) computer hacking of information included any information, a much broader category of computer hacking.

Estimates of other forms of unauthorized access among businesses become more consistent as the manner in which the variables were operationalized becomes more consistent. For example, both the FBI (2005) and Gordon et al. (2006) found that less than 6% of business websites were vandalized, and both studies consistently found that 15% of responding businesses had experienced an intrusion into their computer system (i.e. an offender accessed the computer system without authorization regardless of what information was accessed) (FBI, 2005; Gordon et al., 2006).

Summary

A review of empirical studies of internet-crime reveals that as with traditional forms of crime, the rates at which internet crimes—both internet-related crimes and internet crimes—occur vary across crime types. Of the various forms of internet crime that have been studied, the internet crimes most commonly experienced depends on whether the victims is a business or a private citizen. For businesses victimized by computer crime, the most common victimizations include malware attacks, denial of service attacks and attempts to gain unauthorized access to computer systems. For adult private citizens, the most common type of online victimization is internet-related fraud, online auction fraud and non-delivery of services and/or goods purchased via the internet. For youths, the most common victimizations are exposure to unwanted online sexual images and online sexual solicitations. While a small minority of youth are victims of online harassment, a larger portion of youths harassed online are being chronically harassed. These findings and conclusions are based on a limited number of studies of internet crime, and are therefore tentative at best. However, considering the number of credible and methodologically sound studies that have been conducted, they represent the best that can be expected. Until more studies, relying upon sound methodology, examine the frequency with which internet crimes are committed in America our knowledge base will remain tentative. Only through further research will we be able to construct an accurate picture of internet crime in America.

Internet Crimes Reported to Law Enforcement Agencies

In Chapter One, I discussed several predictions made during the 1970's and 1980's suggesting that the development of the internet would change the nature of crime, and indirectly change the role of police in controlling crime. In order to make a first step towards assessing the

validity of such predictions it is necessary to determine the extent to which police are called upon (or otherwise become aware of) internet crime occurrences. Regardless of the number of internet crimes that occur in America each year, unless those crimes are reported to law enforcement officials, they will remain hidden within the dark figure of crime and will not be addressed by law enforcement agencies. Present indications are that only a very small proportion of internet crimes (regardless of whether the victims are businesses or private citizens) come to the attention of any law enforcement agency and thus remain largely hidden within the dark figure of crime. The following section discusses various findings within the internet crime literature examining the frequency with which various forms of internet crime are reported to law enforcement by discussing the reporting practices of the three types of victims studied: businesses, youths and cyber-stalking victims.

Reporting Practices of Businesses

Studies of internet crimes against businesses routinely find that a relatively large amount of internet crime is not reported to any law enforcement agency. Overall, the FBI (2005) found that 9.1% of all incidents were reported to the police (including federal, state and local agencies). Randala (2004) found even when only the most significant cyber-crime incident experienced is considered, only 13.1% of businesses reported these cyber-crimes to the police. Furthermore, the likelihood that a crime will be reported is dependent on the type of incident in question (Randala, 2004). The findings from studies examining the percentage of internet crimes reported to law enforcement agencies is consistent with a pattern of a direct relationship between the similarity of the crime to traditional forms of crime and the rates at which the crimes are reported to law enforcement. In other words, less traditional the forms of crime are less likely to be reported to police. For example, the two internet crimes most likely to be reported incidents are

fraud and embezzlement. Both of these crimes are very similar to traditional forms of crime. Randala (2004) found that 87.5 % of embezzlement incidents and 47.1% of fraud incidents were reported to the police[21] (p. 4).

As internet crime becomes less like traditional forms of crime, the rates at which they are reported to law enforcement agencies declines. For example, only one quarter of businesses experiencing one or more successful computer intrusions reported the incidents to a law enforcement agency (Gordon et al., 2006). These crimes typically involve a form of breaking and entering or burglary of a virtual commercial structure, thus distinguishing them from more traditional forms of commercial intrusions. Other forms of internet crime (e.g. theft of proprietary information, vandalism or sabotage of network data) involve non-traditional means of committing crimes against non-traditional targets. These are crimes in which no person or physical target has suffered any physical damage or been stolen. Randala (2004) found that a much smaller proportion of these incidents—theft of proprietary information (16.7%) and vandalism and/or sabotage of a business' network data (10.8%)—were reported than more traditional forms of internet crime. Finally, very few incidents involving either denial of service attacks or computer virus attacks neither of which has a traditional crime counterpart and, therefore, are classified as internet crimes for the purposes of this dissertation. Only 12% of denial of service attacks and 5.5% computer virus attacks were reported to police agencies (Randala, 2004, p. 4).

Reporting Practices of Youths

Studies of internet-crimes against youths suggest that victims are extremely unlikely to

[21] Due to missing data, the percentage of cases reported to law enforcement may be significantly higher. No less than 16% of the data in each crime type were coded as missing, and in some categories (e.g. vandalism/sabotage and computer virus attacks) as much as 27% of the data was missing.

report such crimes to law enforcement officials. While many young victims tell someone about their victimization experience, there is a large proportion of internet crime victims who tell no one about the victimization (Wolak, Mitchell and Finkelhor, 2006). For example, in 44% of sexual solicitations, 35% of aggressive sexual solicitations, 52% of instances of unwanted exposures to online pornography and 33% of instances of online harassment suffered by youths in the YISS-2, the victimized youth told no one else about the victimization (Wolak, Mitchell and Finkelhor, 2006).

In the incidents of sexual solicitation, aggressive solicitations, and online harassment that were reported to someone else, the most likely confidante was the youth's friends and/or siblings (Wolak, Mitchell and Finkelhor, 2006). In incidents of unwanted exposure to online pornography the most likely person to whom the youth turned was a parent or guardian (Wolak, Mitchell and Finkelhor, 2006). Overall, only 5% of sexual solicitations, 7% of aggressive sexual solicitations, 2% of instances of unwanted exposure to online sexual images, and 9% of instances of online harassment reported the incident to a law enforcement agency, internet service provider or other authority[22] (Wolak, Mitchell and Finkelhor, 2006).

Reporting Cyber-stalking Incidents to the Police

One of the few indications of the frequency with which cyber-stalking is reported to law enforcement agencies is a study of the New York City Police Department's Computer Investigation and Technology Unit (CITU). In this study, the authors found cyber-stalking was, and had been since the unit's inception, the internet crime most commonly reported to and investigated by the Computer Investigation and Technology Unit (D'Ovidio and Doyle, 2003).

[22] Due to an aggregation bias in the data it is not possible to determine what portion of the cases reported to law enforcement agency, internet service provider or other authority were reported to each type of authority; however, for the purposes of this discussion, the above proportions demonstrate that law enforcement is a rather rare event.

Between January 1996 and August 2000, cyber-stalking accounted for nearly 43% of the cases investigated by CITU (D'Ovidio and Doyle, 2003). These figures suggest that at least in terms of the NYPD Computer Investigation and Technology Unit, cyber-stalking is one of the more reported internet crimes relative to other types of incidents.

Conclusions

In conclusion, the empirical literature of the number of internet crimes occurring in America is extremely limited. Even fewer studies have addressed the extent to which such crimes are reported to law enforcement agencies. Despite the small proportion of internet crimes reported to law enforcement agencies, the findings from a study conducted by the Pittsburgh Division of the FBI suggest that internet crime complaints are distributed across a large proportion of law enforcement agencies. An analysis of the FBI study indicates that 77% of federal, state and local law enforcement agencies in West Virginia and Pennsylvania received complaints about internet crime victimizations (FBI, 2005a). However, without further research addressing the types of crimes reported to law enforcement agencies, our understanding of the types of crimes police are being asked to control will remain limited.

Chapter Three: Literature Review

The Roles of Local Law Enforcement Agencies

The roles of law enforcement agencies have long been a topic of theoretical debate among policing scholars. Scholars have framed the role of local law enforcement agencies in terms of such diverse activities as enforcing the law (Wilson, 1968), preventing crime (Peel in Vila and Morris, 1999), maintaining order (Wilson, 1968; Wilson and Kelling, 1982), organizing and leading the community (Oliver, 2001), being a community advocate (Vollmer, 1919, in Vila and Morris, 1999), serving the community (Wilson, 1968), wielding force on behalf of society (Bittner), and solving problems within the community (Eck and Spelman, 1987; Goldstein, 1979).

Despite the multitude of roles bestowed upon law enforcement agencies, only three have come to represent the "core" roles of local law enforcement agencies (Zhao et al., 2003, p. 700). The first of the three core roles of law enforcement agencies is maintaining order (Zhao et al., 2003; Wilson, 1968). Wilson (1968) claims that order maintenance is one of the most important functions of the police, but also the most challenging roles. Maintaining order within the jurisdiction of a given law enforcement agency requires the police to intervene in situations in which the disruptive behavior is not necessarily illegal and the officer must exercise a great deal of discretion (Wilson, 1968). In addition to maintaining order, local law enforcement agencies are expected to provide a wide array of services to the community, many of which are performed by no other agency (Wilson, 1968). During the course of a given day, a police officer "directs traffic, provides emergency medical aid, gets cats out of trees, checks on the homes of vacation, and helps little old ladies who have locked themselves out of their apartments" (Wilson, 1968, p. 4). Finally, local law enforcement agencies have been charged with the very daunting task of

controlling crime, both through prevention of crime and through reactive response. It is with the crime control role of local law enforcement agencies, specifically in regards to controlling internet crime, which this dissertation is concerned. The most common crime control activity of the police is arresting suspected offenders; however, as will be discussed later in this chapter, the police engage in many different activities in controlling crime. This dissertation is an attempt to articulate the activities in which local law enforcement agencies engage in controlling internet crime.

In addition to the ongoing theoretical debate, there has been a great deal of research examining the roles local law enforcement agencies serve (Burton et al., 1993). This research has primarily focused on the roles of local law enforcement agencies in dealing with traditional problems of society, such as the role of law enforcement agencies in controlling traditional forms of crime. However, the development of the internet and the growing popularity of internet-related activities have created new means for offenders to commit crime, and have created a new venue (e.g. cyberspace) in which offenders can victimize others. Scholars have begun to realize that many of the means by which the police have controlled traditional forms of crime are ill-suited for combating crime in cyberspace (Brenner, 2003). In light of these developments, it is necessary for scholars to re-examine the role of local law enforcement agencies in controlling non-traditional forms of crime, such as crimes committed in cyber-space. The current chapter reviews the empirical literature examining the role of local law enforcement agencies in America in controlling internet crime.

The Role of the Local Police in Controlling Internet Crime

In Chapter One, I discussed the three dimensions of the crime control role of local law enforcement agencies: the prescribed role, the preferred role, and the enacted role. Researchers

have examined each of these dimensions in terms of the role of law enforcement agencies in controlling internet crime; however, these efforts have been few and have primarily focused on law enforcement agencies of all levels (i.e. past efforts have not disaggregated these effects by the different levels of law enforcement agencies). Due to the limited nature of past research efforts, little is known about the three dimensions of the local law enforcement agencies in controlling internet crime. The following sections review the internet crime literature articulating what is known about each of these dimensions of the role law enforcement agencies serve in controlling internet crime. This review begins with the prescribed role of law enforcement agencies.

The Prescribed Role of the Local Police Agencies in Controlling Internet Crime

As discussed in Chapter One, the prescribed role of law enforcement agencies represents "the legally mandated functions set forth by state legislatures in state legal codes" (Burton et al., 1993, p.684). In other words, the prescribed role of the police represents the role the police are "*supposed* to perform" (Burton et al., 1993, p. 684). In terms of internet crime, the prescribed crime control role of law enforcement agencies is composed of two aspects: the various internet-related activities defined as criminal offenses within the criminal statutes, and whether an agency is responsible for investigating internet crime complaints. The following sections discuss each of these aspects, beginning with a discussion of the internet-related crime laws in the state of Ohio[23].

Internet-related Crime Laws in Ohio

Title XXIX of the Ohio Revised Code (ORC) includes all statutes defining specific acts as criminal (ORC §2901.03). These statutes provide the basis upon which local law enforcement

[23] The following discussion is limited to Ohio internet crime laws because the data for this dissertation will be collected from local law enforcement agencies in the state of Ohio.

agencies are authorized to intervene on behalf of the state. Internet crime is defined in two ways within the criminal statutes of Title XXIX of the Ohio Revised Code: either directly in the text of the statute, or indirectly through application of a general crime statute.

Several types of crime are defined as internet crime within the text of the relevant statutes. These statutes specifically mention the internet, or related terms which the ORC specifies as including the internet, as a means of committing the crime. The offenses for which the ORC statute specifies the internet as a means of committing the crime include: accessing a computer or computer system without authorization (ORC §2913.04 and §2913.06), disruption of public services (ORC §2909.04), disseminating harmful materials to juveniles (ORC §), importuning (ORC §2907.07), menacing by stalking (ORC §2903.211), illegally distributing spam email (ORC §2913.421), using a telecommunications device to harass others (ORC §2917.21), distributing a virus (ORC §2909.07), tampering with records (ORC § 2913.42), and passing bad checks (ORC § 2913.11).

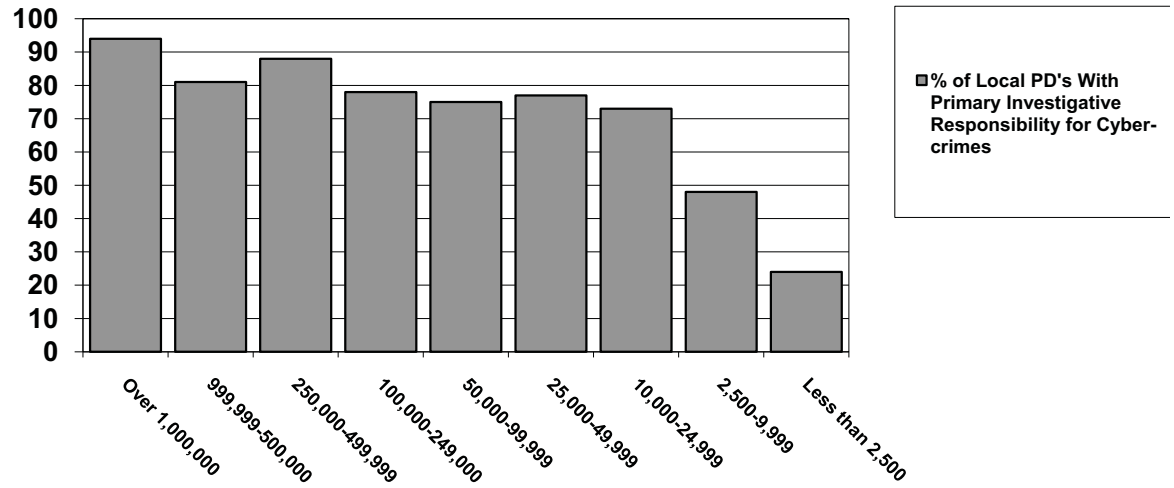
In instances in which the ORC statutes does not mention the internet as a method of committing a specific crime, the crime can still be defined as an internet crime through application of Title XXIX §2901.11 of the Ohio Revised Code. This statute is a general crime statute stating that "a person who, by means of a computer, computer system, or information service, causes or knowingly permits any writing, data, image, or other telecommunication to be disseminated or transmitted into this state [Ohio] in violation of the law of this state" (ORC, §2901.11; Brenner, 2001). This statute, intended to allow Ohio the "broadest possible jurisdiction", provides an indirect means of authorizing local law enforcement agencies to intervene in any case in which the internet is used to commit a traditional form of crime (ORC, §2901.11). While application of ORC §2901.11 makes it technically possible for any act

committed via the internet to be defined as a crime, different crimes are more or less amenable to be committed via the internet. Chapter Four discusses the internet crimes used in this study.

Responsibility for Controlling Crime

The second aspect of the prescribed role of local law enforcement agencies concerns the responsibility for investigating internet-crime. An analysis of the 2003 wave of the LEMAS study indicates that 45% of local police departments, employing three-quarters of all police officers in America, have primary responsibility for investigating complaints about cyber-crime (including both internet crime and computer crime) (Hickman and Reeves, 2006). As shown in Figure 2.1, this percentage varies with the size of the population served by the police department.

Figure 2.1. Percentage of Local Police Departments with Primary Investigative Responsibility for Cyber-crimes by Size of Community Served. (Adapted from Hickman and Reeves, 2006).



The findings from the 2003 LEMAS study data indicate the likely presence of a threshold effect. In local police departments serving less than 2,500 persons, only 24% have primary responsibility for investigating cyber-crimes (Hickman and Reeves, 2006). For those serving populations between 2,500 and 10,000 persons, 48% of local law enforcement agencies have primary investigative responsibilities in cyber-crime complaints (Hickman and Reeves, 2006).

However, once the population served reaches or exceeds 10,000 persons, the percentage of local police departments with primary investigative responsibilities for cyber-crime stays well above 70%, reaching as high as 94% in departments serving 1,000,000 or more persons (Hickman and Reeves, 2006).

The Preferred Role of Local Law Enforcement Agencies in Controlling Internet Crime

While the preferred role of local law enforcement agencies in controlling *traditional* forms of crime has been widely studied (Burton et al., 1993), the preferred role of such agencies in controlling *internet* crime has received much less attention. The preferred dimension of the role of police agencies includes the tasks the citizens expect the police to perform, and the duties the police officers themselves expect to perform[24] (Burton et al., 1993).

Much of our knowledge about the preferred role of the police in controlling internet crime comes from ancillary findings of internet crime research designed to examine other aspects of the internet crime and cyber-crime phenomena. For example, our knowledge of the percentage of crimes reported to law enforcement agencies—an indicator of the number of crimes the complainants of which want the police to become investigate—comes primarily from studies of the number of internet crimes and cyber-crimes occurring in America. Because these findings come from studies primarily addressing other issues, the data are often less than optimal. For example, in studies of the number of cyber-crimes occurring, the findings of the percentage reported to law enforcement agencies is often based on aggregates of all levels of law enforcement agencies, or in some cases aggregates which include both law enforcement and non-law enforcement agencies. As a result of these aggregation biases, we have only a limited understanding of the types of internet crime victims report to law enforcement, and even less

[24] The current study only discusses the preferred role of the public.

understanding of the types of internet-crimes reported to *local* law enforcement agencies.

A recent study conducted by the FBI's Pittsburgh Division examined the types and number of internet-crime related complaints received by law enforcement agencies in Western Pennsylvania and West Virginia. Of the 283 federal, state and local law enforcement agencies participating in the study, approximately three-fourths (77%) of agencies received complaints about cyber-crimes (FBI, 2005a). However, consistent with findings from studies of traditional crime, studies of internet crime routinely find a large portion of the internet crime which occurs is not reported to *any* law enforcement agency. For example, as discussed in the previous chapter, studies of businesses victimized by internet crime or cyber-crime find that no more than 25% of incidents were reported to a law enforcement agency (FBI, 2005; FBI, 2006; Randala, 2001). The 2001 Computer Security Survey Pilot Study found that 35% of the most significant incidents experienced by businesses were reported to law enforcement agencies (Randala, 2001). Similarly, internet crimes committed against juvenile victims, including sexual solicitations (<1% and 5%[25]), aggressive sexual solicitations (2% and 7%), online harassment (1% and 9%) and unwanted exposure to online pornographic material (0% and 2%), are rarely reported to law enforcement (Wolak, Mitchell and Finkelhor, 2006, p. 26).

Some scholars interpret the low rates at which internet crimes are reported to law enforcement agencies as evidence of the police failure to adequately address the problem of internet crime (e.g. Goodman, 1997), while other scholars argue that the low rates at which internet crime victimizations are reported to the police are indications that law enforcement agencies may not be the preferred mechanism for dealing with some forms of internet crime (Warren and Streeter, 2005). Studies of internet crimes committed against businesses find that

[25] The first percentage refers to findings from the YISS, and the second percentage refers to the findings from the YISS-2.

businesses have specific reasons for not reporting such crimes (Randala, 2001; FBI 2006). For example, businesses routinely report that incidents were not reported to law enforcement because of the belief that reporting such crimes would elicit bad publicity for the company resulting in financial loss and loss of trust, or the belief that competitors would use knowledge of the incident against them (Randala, 2001; FBI 2006). Other reasons included seeking alternative legal options (e.g. seeking civil action), or the belief that the police were not capable of providing assistance (Randala, 2001; FBI 2006).

Without further studies of the types of crimes reported to law enforcement agencies, the preferred role of law enforcement agencies in controlling crime will likely remain in the realm of speculation. The current study is one such effort to examine the preferred role of local law enforcement agencies by examining the types of crime complaints which local law enforcement agencies receive. These complaints represent specific requests for police to intervene in instances of internet crime.

The Enacted Role of the Local Law Enforcement Agencies in Controlling Internet Crime

Similar to the other two dimensions of the role of law enforcement agencies in controlling internet crime has been the subject of very few studies; however, it is possible to gain at least a preliminary grasp of the types of activities which local law enforcement agencies use to control internet crime. The following section reviews that which is currently known about the enacted role of local police agencies in controlling internet crime.

Local law enforcement agencies respond to cyber-crime and internet crimes in a variety of different ways. Some agencies investigate complaints of cyber-crime, while others refer such complaints to another law enforcement agency. Some law enforcement agencies use proactive investigation techniques such as sting operations, others do not. Many law enforcement agencies

are supportive of cooperative efforts (such as internet crime task forces); however, very few agencies participate in networks which share information about cyber-crime or participate in security organizations. The following sections of this chapter review the empirical evidence from studies examining the various actions in which law enforcement agencies engage in efforts to control internet crime and cyber-crime.

Investigation and Referral of Cyber-crime and Internet Crime Complaints

A study by the Pittsburgh Division of the FBI found that 77% of law enforcement agencies received cyber-crime complaints, but that only 62% of Law Enforcement Agencies reported actively investigating cyber-crime incidents (FBIa, 2005). It appears that a large portion of law enforcement agencies responding to the survey were ill-equipped to deal with cyber-crime investigations. For example, the vast majority (89%) had neither an investigator assigned to investigate cyber-crimes nor a forensic computer examiner on staff (FBIa, 2005). Only 11% of law enforcement agencies had one or more qualified investigators or examiners, and no agency had more than two such experts (FBIa, 2005). Over half the responding agencies indicated that they did not "typically" collect digital evidence at crime scenes (FBIa, 2005). At first glance, this finding is surprising because of admonitions that digital evidence if collected properly can assist in identifying the offender in internet crimes and, in some cases, may be the only available means of identifying the offender (Wells et al., 2004). However, this finding appears more reasonable when one considers that the FBI Pittsburgh Division study also found that the vast majority of local police departments (95%) indicated rarely or never relying on forensic examinations of digital evidence to advance an investigation or prosecution; and only 13% of agencies surveyed reported spending more than $500 on cyber-crime training in the year

previous to the study[26] (FBI, 2005a).

Among agencies which actively investigate cyber-crime complaints, many relied on outside agencies for computer-related forensic examinations. For example, the majority of such examinations were referred to state police agencies for investigation (FBI, 2005a). Other agencies to which computer-related forensic examinations were commonly referred include the FBI, various county sheriff departments, the Drug Enforcement Administration, and the Secret Service (FBI, 2005a).

Rather than actively investigating cyber-crime complaints, some law enforcement agencies refer complaints regarding internet crime to other agencies. According to data from the 2005 FBI Pittsburgh Study, of those agencies which do not actively investigate cyber-crime, 92% of agencies refer such complaints to another agency (FBI, 2005a). Another 5% of law enforcement agencies not actively investigating cyber-crimes do not refer such complaints to other law enforcement agencies or organizations. The agencies to which law enforcement agencies most commonly refer cyber-crime cases include the state police and the FBI, with well over 135 agencies reportedly referring such cases to these agencies. Agencies to which law enforcement agencies refer cyber-crime complaints to a lesser extent include county police, postal inspectors, district attorneys, Internet Crime Complaint Center, the Secret Service, various high tech crime task forces, local police agencies, the Bureau of Alcohol, Tobacco and Firearms, the Federal Trade Commission, the National Center for Missing and Exploited Children, and the Customs Bureau or Border Patrol (FBI, 2005a).

Arrests for Internet-Related Crime

The activity most commonly associated with the crime control role of local law

[26] The author makes no assumptions or speculation regarding the temporal ordering of these two findings.

enforcement agencies is arresting suspected offenders. However, despite the emphasis placed on the arrest practices of local law enforcement agencies in controlling internet crime, few empirical studies have examined the number of arrests made by local law enforcement agencies in response to internet crime and cyber-crime complaints, and the evidence that does exist indicates that internet crime related arrests are relatively rare events. For example, the National Juvenile Online Victimization Study found that only 385 law enforcement agencies (17%), of the 2,270 agencies participating in the survey, reported making an arrest for one of three internet sex crimes committed against children between the beginning of July 2000 and the end of June 2001 (Wolak, Mitchell and Finkelhor, 2003). These 385 agencies reported making a total of 1,723 such arrests during the one year study period (Wolak, Mitchell and Finkelhor, 2003). Approximately 39% of these arrests involved internet-initiated sex-crime victimizations against identified juvenile victims--approximately half of which involved cases in which strangers initiated contact for the purpose of exploiting a child sexually via the internet, and approximately half of which were initiated by a prior-acquaintance or family members using the internet to further sexual victimizations of a child. Another 36% of the arrests were made for crimes involving the possession and/or distribution of child pornography in which investigators were not able to identify the victims (e.g. police could not identify the children depicted in the images) (Wolak, Mitchell and Finkelhor, 2003). Finally, as will be discussed in the next section, a significant portion of the reported arrests were the result of proactive investigative efforts, such as sting operations in which a law enforcement officer engaged in online activities while posing as a juvenile.

Sting Operations

One of the most publicized activities of law enforcement agencies is the use of sting

operations to capture internet predators. However, many of the accounts publicized in the media focus on isolated efforts of individual agencies, and contribute little to our understanding of the activities of law enforcement agencies in controlling internet crime.

Online sting operations have also proven to be a quite controversial tactic for apprehending offenders committing internet crimes (Tawil, 2000). Much of the controversy involves the question of whether sting operations represent an unfair threat to the suspect's due process rights, such as through entrapping suspects (Tawil, 2000). Other scholars, such as Langworthy (1989) have questioned the overall value of sting operations in fulfilling organizational goals (e.g. transitive and reflexive goals). However, the legality or usefulness of online sting operations falls outside the scope of this dissertation and is mentioned here to demonstrate that this strategy is not universally accepted.

This section reviews an empirical study which, among other things, examined the effectiveness of internet related sting operations for controlling internet sex crimes committed against children. As discussed above, the National Juvenile Online Victimization study surveyed law enforcement agencies about internet-related sex crimes committed against children which ended in arrests within the past year (Wolak, Mitchell and Finkelhor, 2003). Researchers found that of the 1723 arrests made by law enforcement agencies in a nationally representative sample of federal, state, county and law enforcement agencies and internet related task forces, approximately one-fourth were attributable to proactive sting efforts of law enforcement agencies (Wolak, Mitchell and Finkelhor, 2003).

Law Enforcement Participation in Cooperative Efforts

Cooperative investigative efforts appear to garner a high level of support from law enforcement agencies. For example, of the nearly 300 law enforcement agencies surveyed in the

2005 FBI Pittsburgh study, 59% indicated willingness, given the opportunity, to participate in a cyber-crime or internet crime task force (FBI, 2005a). Furthermore, the National Juvenile Online Victimization survey found that of the 1,723 arrests reported by law enforcement agencies involving internet sex crimes committed against juveniles, nearly 80% of the arrests were the result of cooperative investigation efforts between two or more law enforcement agencies of all levels, and 46% of the investigations resulting in an arrests involved three or more such agencies (Wolak, Mitchell and Finkelhor, 2003). In many cases (25%), these investigations resulted in multiple arrests (Wolak, Mitchell and Finkelhor, 2003). In instances in which multiple arrests were made, the vast majority (85%) were state level charges, and although federal agencies were involved in 46% of investigations, only 21% of such investigations involved charges being filed in federal courts (Wolak, Mitchell and Finkelhor, 2003).

The use of cyber tip-lines through which citizens can report internet crimes has become a popular means of connecting law enforcement agencies with non-profit organizations. For example, the cyber tip-line of the National Center for Missing and Exploited Children (NCMEC) was established to "encourage the reporting and investigation of internet child pornography and other online threats to children" (Wolak, Mitchell and Finkelhor, 2003, p. 11). According to the NCMEC, during the 2005 calendar year, the cyber tip-line received a total of 70,760 complaints about online threats to children, including: 64,250 complaints of child pornography, 553 complaints of child prostitution, 205 complaints of child sex tourism, 1,641 complaints of child sexual molestation, 2,664 complaints of online enticement of children, 613 complaints of unsolicited obscene material sent to a child, and 842 complaints of misleading domain names (NCMEC, 2007).

Despite the popularity of cooperative investigative efforts between different law

enforcement agencies and cyber tip-line, it appears that the popularity does not extend to cooperative information sharing networks. According to the FBI, very few of the law enforcement agencies surveyed in 2005 were affiliated with any of several cyber-crime and/or security organizations, including: the FBI InfraGard program, the High Tech Criminal Investigations Association, the Computer Security Institute, the Information Systems Security Association, and the Information Systems Audit and Control Association (FBI, 2005a). Only 10 of nearly 300 law enforcement agencies surveyed reporting participating in any of the above information sharing networks and organizations (FBI, 2005a). This finding is surprising in light of predictions that successful cyber-crime investigations will require the establishment of networks between police departments and other units of the government and agencies within the private sector (Broadhurst, 2003).

Conclusions

This chapter has reviewed the literature concerning the three dimensions of the role of law enforcement agencies in controlling internet crime, including the prescribed role, the preferred role and the enacted role. While scholars have addressed each of these dimensions to some extent, overall very little has been done to articulate the role of law enforcement agencies in controlling internet crime. Even less attention has been given to the role of *local* law enforcement agencies in controlling internet crime. As a result of the dearth of scholarly research addressing the role of the police in the Age of the Internet, we know neither what duties the citizenry expect the police to perform nor the duties law enforcement agencies actually perform. However, the available empirical evidence suggests that, at least for some forms of internet crime, local law enforcement agencies may not be the preferred. The current dissertation is an effort to expand the existing knowledge by articulating the preferred and enacted role of

law enforcement agencies in controlling internet crime.

Chapter Four: Methodology

This chapter discusses the methodology of the current study. First, the three primary research questions addressed by the study are presented. Second, the sampling method used, as well as the sampling frame from which the final sample of cases was drawn, are discussed. Third, the survey instrument is discussed and the operationalization of the dependent, independent and control variables is explained. Finally, the methodological limitations of the present study are acknowledged and discussed.

Research Questions

This study addresses three research questions. Each of these questions has either been insufficiently answered or remains unaddressed by the existing internet crime literature. These unanswered questions represent gaps in our understanding of the police in American society.

The first research question—*What role do communities expect local police agencies to serve in controlling internet crime?"*—concerns the *preferred* role of the police in addressing internet crime. While Burton et al. (1993) include both the expectations of the community and the expectations of the officers within the various law enforcement agencies as components of the preferred role, the current study focuses on the expectations of the community.

In order to answer the above research question, it will be necessary to examine two smaller yet related issues. First, it is necessary to examine the total number of calls for service received by local law enforcement agencies which concern internet crime. Second, in order to avoid an aggregation bias concealing the variety of internet crimes reported it is necessary to examine the volume of various types of internet crimes reported to local law enforcement agencies. This examination would provide not only an indication of whether or not the citizenry expects local law enforcement agencies to address internet crimes, but would also provide an

indication of types of internet crimes citizens consider to be within the responsibility of local law enforcement agencies to address all forms of crimes and provide a examination of the preferred role of local law enforcement agencies in controlling internet crime.

The second research question—"*What is the enacted role of local law enforcement agencies in controlling internet crime?"*—acknowledges the possibility that the *actual* role local law enforcement agencies serve in controlling internet crime may not coincide with the community's *preferred* role of such agencies. In order to answer this question, it is necessary to examine the activities in which local law enforcement agencies engage in their attempts to control internet crime. Two types of police activities are examined. The *reactive* efforts of local law enforcement agencies include any activities police officers use to address internet crimes reported by members of the community or referred to them by other law enforcement agencies. The *proactive* efforts of local law enforcement agencies—including activities initiated by an agency to address a crime before it is committed—are also examined. Through examining both parts of the enacted role of local law enforcement agencies, the author seeks to provide the first articulation of the types of activities local law enforcement agencies actually use to control internet crimes within their jurisdiction.

Finally, it has been argued that organizational structure and other characteristics of local law enforcement agencies are related to the role of such agencies. It is upon these findings that the third research question is formed. The final research question addressed by the present study, and founded on the above findings, asks "*Which organizational and/or structural characteristics of local law enforcement agencies are correlated with variation in the preferred and enacted roles of local law enforcement agencies?".* In order to address this final research question, two types of organizational characteristics are examined. First, a set of variables describing the

manner in which personnel within the department are allocated is examined. The second set of variables examined includes structural dimensions of local law enforcement agencies. The individual sets of characteristics, and the manner in which the various items are operationalized, is discussed in detail in a later section of this chapter.

Data Source

The data used to answer the above research questions were collected from a sample of local law enforcement agencies, in the state of Ohio. The data were primarily collected via a self-administered survey questionnaire mailed to the chief administrators of such agencies. The following section discusses the study population.

Study Population

The sample used in the current study was drawn from the population of all local law enforcement agencies in the state of Ohio. Elements in the population were identified from a list of all local police agencies in Ohio created by the Ohio Peace Officer Training Commission (OPOTC). This list was created pursuant to the requirements of Section 109.761(B) of the Ohio Revised Code. This statute, effective since February 2002, requires any Ohio agencies which appoint or employ any law enforcement officers to "annually provide to the Ohio peace officer training commission a roster of all persons who have been appointed to or employed by the agency or entity as peace officers or troopers in any full-time, part-time, reserve, auxiliary, or other capacity and are serving, or during the year covered by the report have served, the agency or entity in any of those peace officer or trooper capacities" (ORC, 2009). The list of agencies used here was created in 2005—the most recent year for which data was published and, consequently, the first year in which the OPOTC achieved compliance from all agencies in the state. Thus, the sampling frame used for this study was the most current and accurate list of

Ohio law enforcement agencies available at the time.

According to a report prepared by the Ohio Peace Officer Training Commission there were a total of 987 agencies in the state of Ohio which appointed or employed at least one police officer in 2005 (OPOTC, 2005). However, it was necessary to remove some agencies from this list because their function and/or jurisdiction fell outside the scope of agencies with which this dissertation is concerned.

The population of interest for the current study is limited to *local* law enforcement agencies. For the purposes of this dissertation, a local law enforcement agency is defined as either a municipal police department or a county sheriff's department. Maguire (2003) defines a municipal police department as "a general purpose law enforcement agency that responds to calls for service from citizens and enforces a wide-range of state criminal laws and local ordinances" (p. 113). Furthermore, such agencies' jurisdiction will be confined to a city, village or township rather than "a state, a county, a territory, or a specialized district, such as a school of an airport" (Maguire, 2003, p. 113). County sheriff's departments in Ohio are also included in the present study because in rural and unincorporated areas of the state, these agencies function in much the same manner as a municipal police department.

Based on the above definitions, a total of 116 police agencies were removed from the initial sampling frame including state-level agencies and a variety of special purpose law enforcement agencies. The number and types of agencies removed from the OPOTC list is presented in TABLE 4.1 below. After all of the ineligible cases were removed from the sampling frame, a total of 871 local law enforcement agencies—including 783 municipal law enforcement agencies and 88 county sheriff's departments—remained in the population of interest.

Table 4.1 Agencies excluded from the population	
Agency Type	Number of agencies
Police agencies exclusively serving a college or university campus	34
Park police agencies	32
Police agencies exclusively serving a hospital/behavioral health center	26
State-level law enforcement agencies	11
Airport police agencies	3
Transit police agencies	2
Amusement park police	3
Police agencies serving housing authority/veteran's home	2
Railroad police agencies	2
Law enforcement task force	1
Total	116

The 871 law enforcement agencies in the study population include 783 municipal law enforcement agencies and 88 county sheriff's departments serving communities with populations of very different sizes. The distribution of municipal law enforcement agencies by the population serve is presented in Table 4.2 below.

Table 4.2 Municipal law enforcement agencies by population of the community served.		
Population of Community Served	Number of Agencies	Percentage
Very small community (less than 4,000 residents)	442	50.98%
Small community (4,000 to 9,999 residents)	146	16.76%
Medium-sized communities (10,000 to 19,999 residents)	100	11.48%
Large communities (20,000 to 49,999 residents)	64	7.35%
Very large communities (more than 50,000 residents)	29	3.33%
Total	871	***[27]

According to the U.S. Census Bureau (2000a), the 781 municipal police departments included in this study have populations ranging from 70 residents to 711,470 residents. The vast majority (588 agencies) of these agencies serve communities with populations of less than 10,000 persons. One hundred law enforcement agencies serve communities of between 10,000 and 20,000 citizens, and sixty-four law enforcement agencies serve communities with

[27] Due to rounding the percentage total is greater than 100%.

populations of between 20,000 and 49,999 residents and twenty-nine law enforcement agencies which served communities of more than 50,000 residents.

Similar to the municipal law enforcement agencies discussed above, the county sheriff's departments in the sample population serve communities of a wide variety of population sizes. County sheriff's departments in Ohio serve communities ranging in size from 12,806 to 1,393,978 residents. Despite the wide range in the population sizes served, the majority of these departments, over 52%, serve populations of fewer than 60,000 residents, and nearly 70% of departments serving communities under 100,000 residents (U.S. Census Bureau, 2000b). Only 27 sheriff's departments in Ohio serve populations greater than 100,000 residents. Fifteen of these departments serve populations of between 100,000 and 199,999 residents. Twelve departments serve very large counties, those with populations over 200,000 residents, including two departments serving counties with populations of greater than 1,000,000 residents (U.S. Census Bureau, 2000b). Table 4.3 presents the distribution of county sheriff's departments in Ohio across population sizes of the counties served.

Table 4.3 County Sheriff's Departments by population of community served

Population of Community Served	Number of Agencies	Percentage
Less than 30,000 residents	15	17.05%
30,000 to 59,999 residents	25	28.41%
60,000 to 99,999 residents	21	23.86%
100,000 to 199,999 residents	15	17.05%
more than 200,000 residents	12	13.64%
Total	88	***[28]

Sampling Procedure

The sampling procedure used in the current study is rather straight forward. It was decided that the most appropriate way of collecting the data would be to conduct a census of the

[28] Due to rounding, the percentage total is greater than 100%.

entire population. In other words, rather than distribute the survey to a sample of local law enforcement agencies, including both municipal police departments and county sheriff's departments, a survey questionnaire was mailed to each of the chiefs of police of the 783 municipal police agencies and the 88 county sheriffs in the state of Ohio.

There were several reasons underlying the decision to conduct a census of the population rather than collect data from a sample of cases from that population. First, because the finite size of the population (N=871) limited the potential number of cases in the final sample, it was deemed prudent to include as many cases as possible in the data collection effort and thus the decision to survey all cases in the population. In addition to the finite population size, efficiency was also a factor in the decision to conduct a census of the population. The author's original sampling plan was to draw a random sample of cases from two strata in the sampling frame. The sampling frame would initially be stratified by the type of agency (municipal or county). The municipal agencies would then be stratified again based on the size of the population served. However, after calculating the number of cases[29] that would need to be drawn from each of the strata to allow meaningful comparisons to be made across categories, it was evident that, due to the finite nature of the population, a majority of the cases from each strata would need to be sampled. Therefore, it appeared that a census would be a sensible approach to sampling, especially considering the typically small response rates of previous studies concerning internet crime.

The Final Sample

In March 2008, after locating mailing addresses for the police agencies in the final

[29] Using a formula by Yamane (1967) where n is the necessary number of cases to be drawn from a strata is dependent on N, the size of the population and e, the desired level of precision: $n=N/1+N(e)^2$, the total number of cases needed would be 563 of the 871, including 46% of the agencies serving very small communities, 73% of the cases in the small category, 80% of the agencies serving medium sized communities, 89% of the agencies serving large communities and 100% of the agencies serving very large communities.

population, survey questionnaires were mailed via first-class mail to each of the 871 local law enforcement agencies. Of the 871 questionnaires initially mailed, only 69 questionnaires were returned completed. Another 3 completed questionnaires were returned in response to a reminder postcard mailed approximately two months after the initial mailing.

In October 2008, a second copy of the questionnaire was mailed to all agencies which had not yet returned the survey questionnaire. The second follow-up, the third overall mailing, yielded another 41 completed questionnaires, bringing the total number of completed questionnaires to 113—an overall response rate of approximately 13%.

In May 2009, as part of a final follow-up attempt, in an effort to collect data from as many agencies in the population as possible, a very short version of the survey questionnaire was mailed to all agencies which had not yet returned a completed questionnaire. Of the 760 abbreviated questionnaires mailed out, a total of 37 were returned. Overall, after the above mentioned efforts to solicit completed surveys from the 871 local law enforcement agencies in the census, a total of 150 agencies returned completed questionnaires. Furthermore, representatives from two municipalities contacted the author indicating that police departments no longer existed in those communities. Therefore, the overall response rate for the current study, including both the full and abbreviated versions of the questionnaire is approximately 17.3%.

In terms of distribution of the number of municipal law enforcement agencies to the number of county sheriff's departments, the final sample is fairly representative of the population. Of the 869 local law enforcement agencies in the population, 10.1% are county sheriff's departments and 89.9% are municipal law enforcement agencies. Similarly, county sheriff's agencies and municipal law enforcement agencies account for 10.7% and 90.3% of the

response sample, respectively.

Table 4.4 Characteristics of law enforcement agencies in the responding sample		
Characteristic	Number	Percent
Agency Type		
Municipal Police Department	134	89.3
County Sheriff's Department	16	10.7
Total	150	100%
Urbanism		
Urban	26	23.4
Suburban	46	41.4
Rural	39	35.1
Total	111	***[30]
CALEA Certification		
Yes	23	20.9
No	87	79.1
Total	110	100%
College in Jurisdiction		
At least one college in jurisdiction	73	48.7
No college in jurisdiction	38	25.3
Total	111	100%

Survey Instrument

The current study collected data via a self-administered survey questionnaire. This instrument was designed after a careful review of both theoretical discussions and empirical studies contained in three existing bodies of literature described in previous chapters: the internet crime literature, the general policing literature and literature of police organizations. After reviewing these bodies of literature, several key variables were identified and measures were developed with which to transform the variables into survey items for inclusion in the survey instrument which was later mailed to the chief administrators of all local law enforcement agencies in Ohio.

The questionnaire used in the present study is composed of several parts. Part I consists of several questions asking the respondent about general crime statistics in his or her department during the 2006 calendar year. Part II asks the respondent to provide information about the

[30] Due to rounding the reported percentage total does not equal 100%.

volume and types of crime complaints received by his or her agency during 2006. These questions asked the respondent about both traditional forms of crime and crimes committed via the internet. In Part III of the questionnaire, the respondent was asked to provide information about the strategies and/or activities used by his or her department to address internet crime. The strategies addressed by the items in this part of the questionnaire include both proactive and reactive investigation practices as well as various crime prevention strategies and activities. In Part IV, the final part of the survey instrument, the respondent was asked to provide information about various organizational characteristics of his or her agency. Together, the data collected in each of the four parts of the survey instrument would allow the author to answer the three research questions discussed in an earlier section of this chapter.

Variables

Several variables are essential to answering the research questions. These variables include two categories of dependent variables and two categories of independent variables, as well as several variables which control for the possible effects of extraneous factors. Each of these categories of variables is discussed below.

Dependent Variables

There are two categories of dependent variables. One category measures the volume of internet crime complaints received by local law enforcement agencies. In a series of survey items, respondents were asked to provide one of two measures of internet crime depending on which type of data were available to them. Each respondent was asked to provide the number of various forms of internet crimes for which their agency received reports during the 2006 calendar year. If the exact number of reports received was not available, the respondent was asked to provide an estimate of the number of reports received during 2006. Table 4.5 contains a

complete list of the twenty internet crimes included on the survey questionnaire.

Table 4.5 Complete list of internet crimes included on the survey questionnaire
Accessing a computer without authorization (e.g. hacking into a computer system)
Launching a denial of service attack
Dissemination of a computer virus*
Dissemination of SPAM email*
Criminal solicitation*
Sexual solicitation of a minor*
Stalking*
Harassment*
Pandering obscenity or pornography*
Distributing child pornography*
Inciting violence*
Inciting panic*
Making terroristic threats*
Intimidation of another*
Interfering with a custody order*
Commission of a hate crime*
Misusing a credit card*
Fraud via electronic funds transfer*
Identity theft*
Other crime specified by the agency*
*Agencies were asked to only include these crimes if they were committed via the internet and/or email.

While it would have been more precise to ask respondents to provide a simple count of internet crimes, this approach did afford one advantage. It allowed for the collection of data from agencies regardless of whether or not their agency distinguished administratively between internet crimes and traditional forms of crime by allowing respondents to provide an actual count of such crimes if it was available or an estimate of such crimes if an actual count was not available.

The second group of dependent variables measures the degree to which local law enforcement agencies are attempting to control internet crime. Two measures are used. First, the range, or variety, of the crime control efforts of each law enforcement agency in the sample

Table 4.6 Complete list of the crime control responses
Distributing printed pamphlets/brochures about internet crime or internet safety
Distributing online pamphlets/brochures about internet crime or internet safety
Providing links to websites about internet safety
Providing links to websites with information on anti-virus software
Providing links to websites with information on filtering programs
Maintaining a list of problematic websites and/or chat rooms
Regularly monitoring online chat rooms
Conducting, or sponsoring, internet safety presentations
Conducting chat room stings for internet sex predators
Conducting stings targeting distributors of child pornography
Sharing internet crime related information with other law enforcement agencies
Having at least one part-time investigator assigned to investigate internet crimes
Having at least one full-time investigator assigned to investigate internet crimes
Having at least one part-time investigator who specializes in internet crime
Having at least one full-time investigator who specializes in internet crime
Having formally trained internet crime investigators
Investigating complaints from citizens concerning internet crime
Investigating internet crime complaints referred by other agencies
Routinely collecting digital evidence during internet crime investigations
Having an internet crime unit
Participating in an internet crime task force
Distinguishing between internet crime and traditional forms of crime
Maintaining membership in an internet security organization
Providing a phone number (other than 911) for reporting an internet crime or tip
Providing an online means of reporting an internet crime or tip
Other tactic used to control internet crime that was not listed above

was measured. This measure incorporated a series of dichotomous items in which the respondent indicated whether his or her agency engaged in each activity in regards to internet crime. Table 4.6 presents the complete list of the 25 specific crime control activities included on the survey questionnaire, as well as an "other" category for respondents to include any activity in which their agencies engage that was not included on the survey questionnaire. The second measure used is an index score, ranging from 0 to 26, reflecting the overall intensity of effort of

each department to control internet crime in their jurisdiction[31]. Each agency's index score was calculated by simply summing the total number of crime control activities in which each respondent indicated his/her agency was involved. The efforts included in the index score are the same as those used above.

Together, these variables allow the author to provide one of the first articulations of the preferred role of law enforcement agencies in terms of internet crimes (as evidenced by the types and volume of various forms of internet crimes reported to local law enforcement agencies) as well as the enacted role of such agencies (as evidenced by the crime control efforts in which agencies report engaging) in responding to these new forms of crime. The following section discusses the independent variables. These variables were used to explain observed variation in the preferred and enacted roles of local law enforcement agencies in the sample.

Independent Variables

The current study uses several measures of various characteristics of law enforcement agencies to explain observed variation in the dependent variables discussed above. The organizational variables were taken from Maguire's (2003) review of 22 empirical studies which used characteristics of law enforcement organizations as either independent or dependent variables. An additional variable, the age of each law enforcement organization, was taken from other works, such as King (1998) and Maguire (1997).

The independent variables fall into two groups. The first group concerns the ways in which personnel are allocated within the agencies. The second group concerns various structural characteristics of law enforcement agencies. Both of these groups of variables and the ways in which they are operationalized are discussed in greater detail in the following sections.

[31] This cumulative score allows for the addition of one point if an agency provided any other activity that was not listed on the survey questionnaire.

Table 4.7 Independent variables related to allocation of personnel	
Variable	Measure
Civilianization	Number of civilian employees divided by the number of sworn personnel Number of civilian employees divided by the total number of employees
Patrol Concentration	Proportion of all sworn officers who are assigned to patrol duties
Span of Control	Number of sworn officers assigned to patrol divided by the number of sworn officers holding a rank equivalent to, or above, sergeant Estimated number of times during a typical shift in which a patrol officer would be in contact with a supervisor
Administrative Intensity	Proportion of the total number of employees assigned to administrative duties Proportion of the number of sworn officers assigned to administrative duties

The current study includes two measures of an agency's degree of civilianization. First, civilianization is measured as the number of civilian employees divided by the number of sworn personnel (Crank and Wells, 1991). An alternative measure of civilianization—the number of civilian employees divided by the total number of employees (Slovak, 1986; Langworthy, 1986; King, 1999)—is also included.

Civilianization is the practice of "replacing sworn officers with nonsworn personnel for certain positions" (Walker and Katz, 2011, p. 63). Walker and Katz cite three primary reasons for civilianization in police departments—all three of which are relevant to the current study. First, it is thought that replacing sworn officers with civilians would allow those officers more time to engage in "critical police work that requires a trained and experienced officer" (Walker and Katz, 2011, p. 63). Second, the civilians are hired because of some skill that they possess or technical expertise. The skill areas for which civilians are hired to replace sworn personnel is

extremely varied (Travis and Langworthy, 2008). Third, civilianization can be a budgetary tactic designed to free up resources (Walker and Katz, 2011). Civilians, who are often less expensive than sworn officers, can do the same tasks and free up the remaining monies that would otherwise be spent paying a sworn officer a higher salary to do the same job (Walker and Katz, 2011).

It is for the reasons provided above that the degree of civilianization is included in the present study. Specifically, it is expected that departments with higher levels of civilianization will also be more active in combating internet crime. A higher degree of civilianization in a department will free up officers to investigate complaints concerning nontraditional forms of crime (e.g. internet crime). A higher degree of civilianization will also provide the necessary technical and computer skills needed for investigating such nontraditional forms of crime. Finally, civilians will provide the agency with a greater degree of resources that can be expended to pursue such crimes. In short, civilianization is included in the present study because it could exert a potentially important influence on an agency's overall degree of effectiveness and/or activity level in controlling various types of crimes, including internet crimes.

A second variable, the degree to which officers are concentrated within patrol assignments, is measured as the proportion of all sworn officers who are assigned to patrol duties (Slovak, 1986). It is thought that the proportion of officers concentrated in patrol assignments will decrease the number of officers that can be assigned to investigate non-traditional forms of crime, such as internet crime. Also, police patrol is an "extremely expensive, labor-intensive enterprise" and it is thought that increased concentration of officers in patrol assignments would reduce the amount of slack resources that could be spent on investigation of non-traditional forms of crime.

Span of control is measured as the number of sworn officers assigned to patrol divided by the number of sworn officers holding a rank equivalent to, or above, sergeant (Slovak, 1986; Crank and Wells, 1991; Crank, 1990). Secondly, it is measured as the estimated[32] number of times during a typical shift in which a patrol officer would be in contact with a supervisor (Smith and Klein, 1983). It has suggested that an agency with a wider span of control could result in decreased levels of effectiveness in the department and potentially reduce the overall level of activity that the department expends on nontraditional crime control activities (Walker and Katz, 2011).

Finally, the degree to which personnel are concentrated in administrative duties is reflected in two measures. Administrative intensity is operationalized as the proportion of the total number of employees assigned to administrative duties (Langworthy, 1986; King, 1999); and, as the proportion of sworn officers assigned to administrative duties (Ostrom et al., 1978). It is thought that administrative intensity, or administrative concentration, will have a negative effect on the overall level of activity an agency exhibits in terms of crime control activities focused on nontraditional forms of crime. It is thought that administrative intensity will exert an opposite effect than is expected to come with increased levels of civilianization. Whereas civilianization frees officers to engage in other activities, increased levels of administrative intensity will prevent officers from engaging in such activities.

In addition to variables reflecting the manner in which personnel are allocated within local law enforcement agencies, the current study includes several measures of organizational characteristics of those agencies. The age of each agency is measured as the number of years

[32] This item was adapted from Slovak (1983).

since the organization was established[33] (King, 1998; Maguire 1997). It has been suggested that organizational age can have a dramatic effect on other organizational characteristics such as centralization, formalization, and administrative intensity (Maguire, 2003). Older police departments tend to be more formalized and tend to exhibit high degrees of administrative intensity (Maguire, 2003). One the one hand, it is expected that older agencies will be less active in responding to complaints concerning internet crime; however, on the other hand, there is evidence to suggest that older agencies will likely more complex organizational structures with more specialized units to handle specialized forms of crime.

Second, an organization's size is measured in two ways. The two measures of organizational size are the number of actual, sworn, full-time officers and the number of total employees (Kimberly, 1976; Mastofski et al., 1987). The measures of size are included because as Maguire (2003) points out "the majority of the literature supports the notion that larger organizations have more complex structures" (p.74). In terms of the current research, this more complex structure could include specialized units to address internet crime. Also, a link between the complexity of the organizational structure and an agency's size has been tied with a decentralization of decision making (Maguire, 2003). This decentralization of decision making power is likely to result in an organization that is more responsive to the officer's desires and less responsive to the organization's formal managers.

An agency's degree of hierarchical differentiation, or its organizational height, is measured as the number of ranks within that agency (Langworthy, 1986; King, 1999; Crank and Wells, 1991). While the literature suggests that organizational height, the distance from the bottom to the top of the organization, is linked to other measures of organizational structure—in

[33] Age is relative to the point in time from which it is measured. In the current study, age was calculated with 2006 serving as the reference year.

Table 4.8 Independent variables related to structural characteristics	
Variable	Measure
Age	Number of years since the organization was established
Organizational Size	Number of actual, sworn, full-time officers Total number of employees
Organizational Height	Number of ranks
Functional Differentiation	Proportion of all sworn officers who are assigned to specialized, non-patrol duties Number of specialized units within the agency
Spatial Differentiation	Total number of motorized patrol units operating during each of three shifts (day, evening, and night) in a typical 24 hour period

that shorter agencies tend to be smaller agencies and taller agencies tend to be larger agencies—there is evidence to suggest that not all of the variation is accounted for by factors such as size (Maguire, 2003; Langworthy, 1986). In terms of the current study, it is expected that taller agencies will be more active in investigating and responding to internet crime complaints.

There are two measures of functional differentiation. "Functional differentiation is the degree to which the organization divides and assigns its tasks into functionally distinct units" (Maguire, 2003, p. 139). First, functional differentiation within an agency is measured as the proportion of all sworn officers who are assigned to specialized, non-patrol duties (Swanson, 1978); and, alternatively, it is measured as the number of specialized units within each agency (Langworthy, 1986; King, 1999). In terms of the present study, it is suggested that a higher degree of functional differentiation will be associated with a greater level of activity in addressing internet crime complaints including the creation of an internet crime unit to deal with complaints about such crimes.

Finally, spatial differentiation is a measure of the size of the jurisdiction that an agency

serves. A greater degree of spatial differentiation is associated with a larger jurisdiction (Maguire, 2003). For the purposes of the present study, spatial differentiation is measured as the total number of motorized patrol units operating during each of three shifts (day, evening, and night) in a typical 24 hour period (Maguire, 2003). It is included as a variable in this study because it is thought to have "larger" jurisdictions will be less responsive (i.e. active) in responding to internet crime complaints due to the large spatial area for which they are expected to police in terms of traditional forms of crime.

In addition to the two groups of independent variables discussed above, the current study also includes a set of variables to control for extraneous factors. Many of these variables control for the effects of various organizational characteristics which might influence on the findings of the current study. Each of these variables is presented in Table 4.9.

The current study was to include a measure of the minimum educational requirement for new recruits within each agency. Each respondent was asked to indicate his or her agency's minimum educational requirement for new recruits. This variable was to be included as a control variable because of the possibility that agencies with higher proportions of college educated officers may also have more officers who are more familiar with computers. These officers may be more prepared and/or likely to investigate crimes committed via technological means, such as those committed via the internet. It was not possible to include this variable in the analyses because of a lack of variation. Each of the agencies in the responding sample indicated that the minimum requirement for employment was a high school education.

The study controls for the possible influence of two demographic characteristics of an agency's officers. Both the proportion of officers who are female and the proportion of officers who are a minority are included as control variables. These are included for two reasons. First,

a higher proportion of female and/or minority officers within an agency may be indicative of an innovative law enforcement agency. Such an agency may also be innovative in other ways such as investigating non-traditional forms of crime (e.g. internet crimes). Second, an agency with a higher proportion of female and/or minority officers may have made changes to its hiring practices in order to select officers who are more representative of the community served. Such an agency may be more responsive to the community in other ways as well. For example, it may be more likely to consciously match its enacted role with the preferences of the community (e.g. be more involved in internet crime complaints).

Table 4.9 Independent variables, Controls

Variable	Measure
Education Requirement	Minimum educational requirement for new recruits
Officer Demographics	Proportion of officers who are female Proportion of officers in each agency who are minority
Agency Certification	Dichotomous measure (0=no, 1=yes) indicating whether each agency is certified by CALEA.
Collective Action	Dichotomous measure (0=no, 1=yes) indicating whether each agency has a local chapter of a fraternal organization Dichotomous measure (0=no, 1=yes) indicating whether officers in each agency have the capacity for collective bargaining
Urbanism	Whether each agency serves a rural, suburban or urban jurisdiction
NIBRS Participation	Dichotomous measure (0=no, 1=yes) indicating whether an agency participates in the NIBRS program
Slack Resources	Proportion of budgetary expenditures which were non-salary related

The current study controls for whether an agency is accredited by the Commission of Accreditation for Law Enforcement Agencies (CALEA), the capacity for collective bargaining, the presence of a local fraternal chapter, the urbanism of the agency (i.e. whether the agency

primarily serves a rural, suburban or urban area). These variables are included as substitutes for a professionalism variable. The variables are included in an effort to control for the following possibilities: that accredited agencies and/or agencies in more urban areas may be more likely to investigate non-traditional forms of crime, and agencies in which officers have access to collective bargaining and/or a local fraternal chapter may be more responsive to line officers and less responsive to community demands.

The current study also controls for whether each agency is compliant with the move towards the National Incident Based Reporting System (NIBRS). An agency's NIBRS compliance is included as a control variable because of two items included on the NIBRS incident form. The NIBRS incident form includes an item asking officers to indicate whether a computer was used to commit a crime and another item asking officers to indicate whether a computer was the target of a recorded crime (Kowalski, 2002). Whether an agency is NIBRS compliant is included as a control variable because of the possibility that such agencies may be more likely to distinguish between internet crime and traditional forms of crime for record keeping purposes—a finding which could affect the accuracy of their answers relative to other agencies in the sample.

Finally, two variables—the amount of slack resources (e.g. the percentage of budgetary expenditures which were non-salary related) and an agency's share of their local budget (e.g. the percentage of the municipal/county budget that goes to the agency)—are included as a means of measuring an agency's financial preparedness to respond to internet crime complaints. For example, agencies with greater slack resources, or agencies receiving a larger share of their local budget, may be better prepared, in terms of financial requirements, to combat internet crime.

Many of the above measures have never been collected in regards to internet crime and

local law enforcement agencies. It is for this reason that studies such as this are needed so; however without a strong foundation of prior research upon which to build, there are issues which could threaten the validity of this study's findings. The following section discusses the major strengths and weaknesses of the current study.

Strengths and Limitations

In many ways, the current study is an improvement over the designs used in prior research attempts; but, as with any research endeavor, there are still limitations to the current study. The following section discusses both the strengths and limitations of this study.

One methodological improvement of the current study is its focus on *local* law enforcement agencies in *one* statewide jurisdiction. There are two distinct advantages of this approach over the approaches used in past research efforts. First, the author can limit findings to local law enforcement agencies. Past efforts have included agencies from several levels of law enforcement in the same sample and, therefore, have been unable to parcel out what role agencies at various levels serve in controlling crimes committed via the internet. Second, by limiting the sample to one statewide jurisdiction, the current study eliminates the confounding effects of the state-to-state differences in how acts committed via the internet are defined across agencies in the final sample.

A second improvement of the current study, offered by the inclusion of a wider range of internet crimes on the survey instrument, is an improved potential for understanding the role of local law enforcement agencies and how that role differs from one type of internet crime to another. Past studies of internet crime have limited their inquiries to a very small number of crimes. The current study includes a much broader list of crimes which can all be committed via the internet thereby allowing a more accurate estimate of the volume of internet crimes reported

to local law enforcement agencies and a more complex examination of the role local law enforcement agencies serve in combating different types of internet crimes.

While the current study includes a much broader list of crimes than used in previous studies, the current study relies on a much more limited and precise definition of internet crimes. In the current study, the term internet crime only includes crime which is either committed or facilitated via the internet. Past research efforts have often included crimes not actually committed or facilitated via the internet and have likely resulted in exaggerated and/or inflated estimates of the occurrence of internet crime. This more precise definition of internet crime would likely present a more accurate estimate of the occurrences of internet crimes and provide a much more realistic view of internet crime reported to local police agencies.

Finally, the current study uses more sophisticated techniques of data analysis than those used in the bulk of the studies conducted to date. Most of the statistical analyses conducted in prior studies of internet crime have been descriptive at best, relying heavily on frequency distributions and simple graphs. Furthermore, few of the prior studies of internet crime have used tests of statistical significance in the presentation of their findings; therefore, it is impossible to determine whether the findings are statistically significant or merely chance fluctuations in the data. In short, most of the prior research in the area of internet crime has been descriptive, at best; and has often produced findings which may or may not be due to chance. The current effort seeks to not only describe levels of each law enforcement agency's effort, but also to identify significant correlates of those levels of effort.

While the author has attempted to develop the strongest possible research design, there are several limitations of the current study. Some of these limitations threaten the internal validity of the study, thus posing a threat the accuracy of the findings. Other limitations threaten

the external validity of the findings, and thus limit the ability to generalize findings beyond the study's sample. Each of these types of limitations is discussed below.

One limitation of the current study concerns the use of measures which are less-than-optimal. Due to the scarcity of empirical research examining the enacted and/or preferred roles of local law enforcement agencies in controlling internet crime and the organizational correlates of crime control activities in regards to complaints about internet crimes there is little basis guiding the selection of appropriate measures. Also, the current study uses a very limited measure of only one facet of the preferred role of local law enforcement agencies in controlling internet crime—the citizens' preferences as evidenced through crime complaints made to local police agencies. Thus the views of local law enforcement officers concerning the preferred role in combating internet crime remain unexamined.

A second limitation of the present study concerns the small size of the responding sample. Two factors related to the present study may have resulted in the fairly low response rate to the survey questionnaire. First, the nature of the present study may have influenced the response rate. Studies concerning cybercrime and/or internet crime have historically reported lower response rates than other studies of crime; however, surveys of law enforcement agencies report a slightly higher rate of completion. The response rate of the current study is consistent with response rates of the cyber-crime and/or internet crime studies reviewed in Chapter 2. Second, the data collected for the current study may have resulted in the relatively low response rate. These data are not data routinely collected by police departments and as such may not be readily available to survey respondents. While every attempt was made to use measures which were available, or fairly easy to collect, it is possible that the sort of data requested may have inadvertently deterred administrators in some of the agencies from completing the questionnaire.

The small size of the responding sample poses several problems. A small sample introduces the possibility of error. Another limitation of this study also concerns the relatively small sample of cases—the small number of cases results in a limited number of degrees of freedom. This limited number of degrees of freedom limits the use of sophisticated statistical models. Ideally, one would like enough degrees of freedom to allow the construction of various multivariate regression models which could calculate the effect of each independent variable on the dependent variables while simultaneously controlling for the effects of all other independent variables included in the model.

A third limitation of the present study is consistent with much of the internet crime literature; the use of cross-sectional data. While cross-sectional data is informative and provides researchers with a snapshot of a phenomenon at a particular time (e.g. the role of local law enforcement agencies in controlling internet crime), the use of cross-sectional data is not suited to tests of causality. Without data collected at multiple points in time, one cannot establish the temporal order in which the hypothesized cause and effect occur. Therefore, the data used in the current study are not suited to making statements about causation between independent variables and dependent variables.

There are also issues within the present study which threaten the external validity of the findings from the current study and therefore, limit the ability of the author to generalize beyond the sample included in the present study. First, the current study is limited to a single state. While the decision to limit the sample of local law enforcement agencies in this study to a single statewide jurisdiction aids in minimizing confusion over differences in legal definitions of internet crime, it could be argued that this decision also limits the ability to generalize the findings beyond the sample used in the current study. However, King (2009) argues that Ohio is

a “microcosm of America” (p.7). According to King (2009):

> “Politically, Ohio has consistently matched the electoral mood of the nation since the 1980s (Tuchfarber, 1988). Census data indicate that Ohio is more similar to the U.S. average than the other 49 states (and Washington, D.C.) in median income and proportion of people below poverty and is second only to Texas in similarity to the United States in terms of Black population (in 2006). Applegate (1997) contends that Ohio is like the United States in “percent of urban and rural areas, percent of the population that is African American, median age, per capita income, percent living below the poverty level and the unemployment rate” (p.97) (King, 2009, p. 7).

In light of this argument it seems that the location selected is not a not a factor that would challenge the ability to generalize beyond the current sample.

Second, the current study is likely limited by the era in which it will be conducted. Based upon the speed with which the internet developed and the growth in its popularity, it is possible that the use of various crime control efforts among local law enforcement agencies may also show significant growth over the next several years. As more and more local law enforcement agencies begin to adapt to complaints about crime committed via the internet, the findings of this study will likely become outdated. Thus, it will be necessary to conduct follow-up assessments of the role that local law enforcement agencies serve in controlling internet crime.

Despite the above limitations, the current study makes a significant contribution to the policing literature by beginning the process of rectifying a significant oversight in the empirical literature by articulating the current role of local law enforcement agencies in controlling internet crime. Furthermore, the present study will enhance scholarly understanding of the role of local police agencies in controlling crime by providing a more sophisticated statistical data analysis than those conducted in past studies which have been descriptive, at best.

Conclusion and Summary

This chapter has detailed the methodological design to be used in the current study. The current study examines three research questions. These research questions can be summarized as

follows:

> **Question 1:** What is the preferred role of local law enforcement agencies in controlling internet? Specifically, which types of internet crimes do citizens expect local law enforcement agencies to control?
>
> **Question 2:** What is the enacted role of local law enforcement agencies in controlling internet crime? What actions are local law enforcement agencies currently taking in response to reports of internet crime victimizations?
>
> **Question 3:** Which organizational characteristics are statistically significant correlates of either the preferred or enacted role of local law enforcement agencies in controlling internet crime?

The current study attempted a census, in which every agency in the population was included in the sample. The population used in the current study was a list of all local law enforcement agencies, including both municipal police departments and county sheriff's departments in the state of Ohio in 2005. At that time, there were a total of 987 law enforcement agencies, including 783 municipal law enforcement agencies serving villages, towns, cities or townships, and 88 county sheriff departments. By limiting the sample to these two types of law enforcement agencies, the current study overcomes a limitation of prior research. Prior studies have included all levels of law enforcement agencies: therefore, these studies have been unable to disaggregate findings by level of law enforcement agency.

The current study uses a number of independent, dependent and control variables in answering the research questions discussed above. The independent variables, primarily drawn from a review of 22 studies conducted by Maguire (2003) and the work of King (1998; 1999), will be used to explain observed variation in both the number of internet crimes received by local law enforcement agencies, and the response of such agencies to those reported crimes. The independent variables to be used fall into three categories: variables reflecting the manner in which personnel are allocated within departments and organizational characteristics.

Finally, this chapter discussed various limitations of the current study which threaten both the internal and external validity of the findings. However, there are several improvements offered by the current study over prior research. For example, the current study limits the unit of analysis to a single level of law enforcement agencies. By focusing on local law enforcement agencies, including municipal police departments and county sheriff departments, the current study is able to overcome an aggregation bias, present in many previous studies, which prevented the authors from parceling out the efforts of local law enforcement agencies and other levels of law enforcement. Furthermore, the current study includes a wider range of internet crimes than has been used in previous studies, thus allowing a more complete understanding of the *preferred* role of local law enforcement agencies in controlling internet crime. The current study also includes a wider range of possible responses of local law enforcement agencies allowing for a more complete analysis of the *enacted* role of local law enforcement agencies in controlling internet crime.

In conclusion, the current study seeks to articulate the role of local law enforcement agencies in controlling internet crime. In articulating this role, the study builds upon prior research and explores aspects of the role of local law enforcement agencies which have not been previously addressed. Prior research has not adequately explored the role of local law enforcement agencies in regards to internet crime. This represents a significant oversight in the policing literature. It is imperative that scholars begin to rectify this oversight by examining the both the preferred and enacted roles of local law enforcement agencies in controlling internet crime, and by examining the factors which are correlated with both of these roles. The current study represents a significant first step towards completing this important task and developing a fuller understanding of the role of local law enforcement agencies serve in controlling various

forms of internet crime.

The next chapter discusses the manner in which the present data were analyzed and presents the findings of this study. The findings are presented in three sections. First, the preferred role of the police is examined. Second, the enacted role of the police in responding to internet crime complaints is discussed. The enacted role is not only examined in terms of the types of activities in which local law enforcement agencies engage in addressing citizen complaints concerning internet crime, but is also in terms of the overall activity of local law enforcement agencies to address complaints about such crimes. Finally, the chapter discusses the ability of contingency theory to explain observed variation in the enacted role of the police (i.e. the overall activity of agencies) in responding to internet crime complaints.

Chapter Five: Findings

This chapter presents the findings of the current study examining the role local law enforcement agencies serve in controlling internet crime. In the first section of this chapter, the preferred role of the police, as defined by the citizenry served, is examined. In the second section, the actual role of local law enforcement agencies in controlling internet crime is examined. Finally, an examination of the degree to which the response of local law enforcement agencies to internet crimes can be explained by organizational and environmental factors, drawing upon a contingency theory perspective, is presented.

Part I: The Preferred Role of Local Police Agencies

This section addresses the following research question: what is the preferred role of local law enforcement agencies in controlling internet crime? This research question is examined in several stages. The first stage of the analysis examines whether or not local law enforcement agencies in the responding sample were called upon, during the 2006 calendar year, to address internet crimes occurring within their jurisdictions. The second stage of the analysis examines a related but conceptually distinct issue by identifying the specific types of internet crimes the citizenry places within the investigative bailiwick of local police agencies. In the final stage of the analysis, the bivariate correlates of the volume of internet crimes reported to local law enforcement agencies are examined as a means of explaining the preferred role of local law enforcement agencies in the responding sample.

As discussed in the previous chapter, the chief administrators of all 871 local law enforcement agencies in Ohio were mailed a survey questionnaire in which each respondent was asked to provide a count of the various types of internet crimes reported to his/her agency during the 2006 calendar year. Representatives from 113 of the 871 local law enforcement agencies

returned completed questionnaires. After two more mailings, non-responsive agencies were mailed a shortened-version of the questionnaire. Representatives from 37 agencies completed and returned the shortened-version of the survey questionnaire. The findings presented in this chapter are derived from the responses provided by the 150 agencies in the population that completed and returned one of these two questionnaires.

Internet Crime Reporting to Local Police Agencies

Based on the responses provided by agency representatives in the responding sample[34], internet crime *is* an issue which the citizenry calls upon local law enforcement agencies in Ohio to address. Examining Table 5.1 below, approximately 69% of the agencies completing the full questionnaire reported receiving *at least one* complaint concerning internet crime in 2006; and, approximately 84% of the agencies returning a shortened version of the questionnaire reported receiving *at least one* internet crime complaint in the past[35]. The remaining agencies (n=41) in the responding sample either reported receiving no internet crime complaints or failed to provide an answer to the question[36].

Table 5.1 Agencies in the responding sample receiving at least one internet crime complaint

	Full Questionnaire		Short Questionnaire	
	Number	Percent	Number	Percent
Received a complaint in 2006	78	69.03	---	---
Received a complaint ever	---	---	31	83.78
No complaint received or missing	35	30.97	6	16.22
Total	113	100	37	100

[34] Of the 150 agencies in the responding sample, a total of 113 agencies returned the full survey questionnaire and another 37 agencies returned a shortened version of the survey questionnaire which was distributed to agencies which had not responded to 3 prior mailings including two survey questionnaires and a reminder postcard.

[35] The shortened version of the survey did not limit respondents' answers to the 2006 calendar year.

[36] A design problem in the section asking respondents to indicate the number of internet crime complaints received provided some confusion in coding the data. In some cases, it was not possible to determine whether a respondent left an item blank was indicating that no such crime complaints were received or was not providing an answer at all. Therefore, questionnaires in which the respondent did not indicate a count of the number of internet crimes (i.e. left that section of the questionnaire blank) were coded as no reported internet crime complaints. This will provide a conservative count of the number of internet crime complaints received by the local police departments in the sample.

Overall, nearly three-quarters (72.6%) of the agencies in the responding sample had been called upon *at least once*, either during the 2006 calendar year or at some other point in the past, to address an internet crime complaint. Later sections of this chapter will discuss the volume of such calls and the variety of crime complaint types.

Characteristics of agencies receiving at least one report of internet crime

An analysis of the results of a series of bivariate logistic regression analyses identified statistically significant relationships between several independent variables and the likelihood that an agency received at least one internet crime complaint in 2006. Each of these bivariate relationships is discussed below.

Prior to presenting the findings, it should be noted that the small sample size in the present study creates a bias against rejection of the null hypothesis in tests of statistical significance. In the interest of identifying significant differences and considering that the purpose of the present study is largely exploratory, the author has chosen to report a lower standard of statistical significance than is conventional in social science research. The author realizes that while this choice *decreases* the risk of committing a Type II error (i.e. failing to reject the null hypothesis when a real relationship does exist), this choice *increases* the possibility of committing a Type I error resulting in a false positive. It is therefore important to exercise caution in the interpretation of the findings presented in the current dissertation. As such, both the reduced level of significance and the more conventional levels of significance are reported.

Table 5.2 Bivariate predictors of an agency receiving at least one internet crime complaint in 2006						
	B	SE	Wald	df	Sig	Exp (B)
Civilianization 1	-3.729	1.640	5.172	1	.023**	.024
Civilianization 2	-2.932	1.737	2.851	1	.091*	.053
Patrol Concent. 1	-1.513	.709	4.552	1	.033**	.220
Vertical Diff. 1	-.381	.159	5.706	1	.017**	.683
Medium Height	1.157	.422	7.523	1	.006***	3.180
Very Small Pop	-1.511	.498	9.204	1	.002***	.221
Suburban Agency	.878	.452	3.777	1	.052*	2.407
College/University	.955	.484	3.902	1	.048**	2.599
Collective Barg.	1.182	.430	7.546	1	.006***	3.262
						* p≤ .10 ** p≤ .05 *** p≤ .01

Examining Table 5.2, four of the independent variables are negatively related to an agency having received an internet crime complaint in 2006. The two measures reflecting the rate of civilianization within each agency—the ratio of the number of full-time civilian employees to the number of full-time sworn officers and the ratio of the number of civilian employees to the total number of employees—were both inversely related to an agency having received at least one internet crime complaint during the 2006 calendar year ($p < .05$ and $p < .10$, respectively). The value of the Exp(B) indicates that for each 1 unit increase in the ratio of the number of full-time civilian employees to the number of full-time sworn officers the odds of an agency having received an internet crime complaint in 2006 are 0.024 times lower. For the second measure of civilianization, a 1 unit increase in the ratio of the number of civilian employees to the total number of employees results in odds of an agency having received an internet crime complaint in 2006 are 0.053 times lower.

In addition to the measures of civilianization, two other measures are inversely related to

the odds of an agency having received an internet crime complaint in 2006. Examining Table 5.2, size of the population an agency serves is related to the number of internet criem complaints received in 2006, but only for agencies serving very small populations. Agencies that reported serving a very small population were .221 times less likely to have received an internet crime complaint in 2006 ($p < .01$) than were agencies serving populations of any other sizes. Similarly, both patrol concentration, measured as the proportion of all sworn officers assigned to patrol duties, and vertical differentiation of an agency, measured as the number of ranks in an agency, were negatively related to an agency having received an internet crime complaint in 2006 ($p < .05$ for both measures).

Whereas the height of an organization measured as the number of ranks in an agency are negatively related to the odds of an agency having received an internet crime complaint in 2006, an alternative means measuring of height provides some further information on that relationship. When vertical differentiation is measured as two dummy variables representing agencies that are tall (those with more than 7 ranks) and agencies that are medium height (those with between 4 and 6 ranks) only the variable representing organizations of medium height is significant. The results the bivariate logistic regression model indicates that for an agency of medium height the odds that the agency received an internet crime complaint in 2006 is 3.180 times *greater* than for either short or tall agencies. Consequently, the dummy variable reflecting a tall agency was not statistically significant.

Three other variables were related to the likelihood that an agency received an internet crime complaint in 2006. As presented in Table 5.2, the odds of an agency having received an internet crime complaint in 2006 were 2.599 times higher for agencies that reported the presence of a college or university within their jurisdictions, 2.407 times higher for agencies in suburban

areas and 3.262 times higher if the agency reported that its officers had access to collective bargaining.

The Volume of Internet Crimes Reported to Local Law Enforcement Agencies

The survey questionnaire asked each respondent to provide a count of the number of internet crime complaints his/her agency received during the 2006 calendar year. As discussed above, approximately 69% (n=78) of the 113 agencies returning the survey questionnaire received *at least one* internet crime complaint during the 2006 calendar year. The present section of this chapter expands on the above analysis by examining the number of complaints received by the agencies in the responding sample.

Overall, the agencies in the responding sample received a total of 6167 internet crime complaints during the 2006 calendar year[37]. The first column of Table 5.3 presents the measures of central tendency for the number of internet crime complaints received by 113 local law enforcement agencies in the responding sample. The mean number of internet crimes received by local law enforcement agencies in the responding sample was 54.58.

Table 5.3 Measures of central tendency using full sample and using subsample of cases

	All cases	At least one complaint
Number of Cases	113	78
Mean	54.58	79.06
Median	11	21
Std Deviation	137.958	160.381

Comparing the first and second columns of Table 5.3, it is clear that the values of the measures of central tendency depend largely on whether the agencies receiving no internet crimes in 2006 are included in the analysis. When the 35 agencies that received no internet crime complaints in 2006 are excluded from the analysis both the skew of the distribution and

[37] This figure only includes the data provided by those responding to the full survey questionnaire. Inclusion of the data provided by those responding to the short version would be problematic in that the questions on the short version of the survey questionnaire did not limit the time frame of interest to the 2006 calendar year.

the measures of central tendency, especially the mean number of crimes reported, are greatly affected. The revised value of the mean ($\bar{x}$=79.06) represents an increase of almost 24.5 internet crime complaints per agency. While the revised values of the median exhibits a less dramatic change than is evident between the values of the mean, they *are* affected by the exclusion of the cases receiving no internet crime complaints in 2006. With the exclusion of these cases, the median increases from 11 to 21. The revised measures of central tendency are more representative of the present research concerns by providing a much more accurate snapshot of the data of interest.

Because it was thought unlikely that all local law enforcement agencies would be able to provide an accurate count of the number of internet crime complaints, the survey questionnaire was designed in such a way as to give respondents two options for providing the requested data. Respondents who *could* provide accurate counts of the number of internet crime complaints reported in 2006 were asked to do so. If a respondent *could not* provide an accurate count of the number of internet crime complaints received in 2006 he or she was asked to provide an estimated number of such complaints received[38]. The following section examines the number of internet crime complaints received by local law enforcement agencies using these two measures.

Of the 6167 internet crime complaints received by agencies in the responding sample, 1370 were reported as accurate counts (or AC complaints) of such incidents by the respondents. Examining the first column of Table 5.4, the AC complaints accounted for approximately one-fourth (22.2%) of the total number of internet crime complaints agencies in the responding sample reported receiving in 2006. These 1370 AC complaints were reported by 39 of the 78 agencies in the subsample of cases discussed above. The number of AC complaints agencies

[38] While the author realizes that the inclusion of this second option leaves room for measurement error, this measure was included on the survey questionnaire in order to obtain information from as many police departments as possible.

reported receiving in 2006 ranged from a low of 1 internet crime complaint to a high of 315 such complaints, with 50% of agencies reportedly receiving 6 or less internet crime complaints and the mean number of internet crime complaints received was 35.13 complaints per agency.

Table 5.4 Comparison of the AC Complaints, EC Complaints and total complaints received by Agencies			
	Accurate Counts	Estimated Counts	All Counts
Number of complaints	1370	4797	6167
Number of agencies reporting	39	56	78
Mean	35.1282	85.6607	79.0641
Median	6.0000	32.5000	21.0000
Std. Deviation	160.381	139.557	74.720
Range	314	670	888
Minimum	1	5	1
Maximum	315	675	889

The remaining 4797 internet crime complaints reported by agencies in 2006 were estimated counts (or EC complaints) provided by the responding agencies. The second column of Table 5.4 shows that the EC complaints received by 56 agencies in the responding sample accounted for over two-thirds (77.78%) of the total number of internet crime complaints received by local law enforcement agencies. The estimated number of internet crime complaints received by individual agencies demonstrated a great deal of variation. The number of EC complaints received by local law enforcement agencies ranged from a minimum of 5 complaints to a maximum of 675 such complaints--with over half of the agencies reported less than 33 internet crime complaints.

Comparing the first two columns of Table 5.4, it is observed that the mean number of EC complaints received ($\bar{x}$=85.6607) was much higher than the mean number of internet crime complaints received by the AC agencies in the responding sample. Furthermore, the median number of internet crime complaints received by EC agencies was also much higher than for the AC agencies.

Variation in the volume of internet crime complaints received

The volume of internet crime complaints received by the individual local law enforcement agencies in the responding sample during the 2006 calendar year varied greatly, ranging from no internet crime complaints to 889 internet crime complaints. Table 5.5 presents the number of internet crime complaints received by agencies in the responding sample. Of the 113 agencies in the responding sample, 78 agencies reported receiving at least one internet crime complaint during the timeframe of interest; however, most of these agencies received relatively few internet crime complaints. Over 50% of the responding agencies who received an internet crime complaint reported receiving no more than 30 complaints concerning an instance of internet crime.

Table 5.5 Number of complaints received by agencies that received at least one complaint (n=78)

	Number	Percent
1-10 complaints	21	26.9
11-20 complaints	17	21.8
21-30 complaints	5	6.4
31-100 complaints	23	29.5
101-500 complaints	8	10.3
More than 500 complaints	4	5.1

However, as shown in Table 5.5, there is a much greater degree of variation in the number of internet crime complaints received by the agencies in the upper half of the distribution. The number of internet crime complaints received by these agencies ranged from 31 to 889 complaints. Of the remaining agencies in the responding sample, 23 agencies (29.5%) received between 31 and 100 complaints; 8 agencies received between 101 and 500 complaints (10.3%); and 4 agencies (5.1%) received between 500 and 889 internet crime complaints in 2006.

Explaining the Number of Internet Crime Complaints Received

An examination of the bivariate correlates of the volume of internet crime complaints received by local law enforcement agencies in 2006 reveals few statistically significant correlations[39]. A discussion of the variables found to be significantly related to the number of internet crime complaints received by local law enforcement agencies follows.

Examining Table 5.6, only one of the structural characteristics of police agencies was a significant correlate of the number of internet crime complaints received in 2006. Tall agencies are associated with a greater number of internet crime complaints ($p < .05$).

Similarly, only one of the measures of personnel allocation in local police agencies was significantly related to the number of internet crime complaints received in 2006. Agencies with higher percentages of female officers tended to receive a greater number of internet crime complaints in 2006 ($p < .10$).

Five other measures of organizational characteristics were related to the number of internet crime complaints received in 2006. Agencies with a college or university in their jurisdiction tended to receive a greater number of internet crime complaints in 2006 ($p < .01$). Similarly, agencies that had been certified by CALEA tended to receive a greater number of internet crime complaints in 2006 ($p < .01$). The size of the population served was related to the number of number of internet crime complaints an agency received in 2006. However, this finding is only relevant for agencies serving very large populations ($p < .05$), which tended to receive a greater number of internet crime complaints, and for agencies serving very small populations ($p < .01$) which tended to receive significantly fewer complaints concerning internet crime in 2006. Finally, agencies created between 1900 and 1950 tended to receive fewer internet

[39] Pearson Product Moment Correlation Coefficients are presented for metric independent variables. For nominal dependent variables the value of a Point Biserial is provided as a measure of association.

crime complaints in 2006 than agencies created before 1900 or after 1950 ($p < .05$).

Table 5.6 Significant Bivariate Correlates of the Number of Internet Crime Complaints Received		
		Number of Internet Crime Complaints Received
Tall Agency (0,1)	Point Biserial	.195
	Significance (2-tailed)	.039**
	N	113
Date Agency Created 1900-1950 (0,1)	Point Biserial	-.214
	Significance (2-tailed)	.048**
	N	86
CALEA Certified Agency (0,1)	Point Biserial	.396***
	Significance (2-tailed)	.000
	N	110
College or University in Jurisdiction (0,1)	Point Biserial	.315
	Significance (2-tailed)	.001***
	N	111
Very Small Population Served (0,1)	Point Biserial	-.186
	Significance (2-tailed)	.048**
	N	113
Very Large Population Served (0,1)	Point Biserial	.301
	Significance (2-tailed)	.001***
	N	113
Percentage of Officers Who are Female	Pearson Correlation	.172
	Significance (2-tailed)	.069*
	N	113
		* $p \leq .10$ ** $p \leq .05$ *** $p \leq .01$

The relationship between the level of government at which an agency operates (i.e. municipal or county) and the number of internet crime complaints received warrants some examination and discussion. While a police agency's designation as county or local agency was not a significant correlate of the number of complaints received in 2006, a rather odd pattern was detected in the data. The county sheriff departments in the responding sample received a disproportionately larger number of complaints regarding internet crime in 2006.

Table 5.7 Number of internet crime complaints by level of government

	Agencies		Complaints Received			
	Number	Percent	Number	Percent	Mean	Std. Deviation
Municipal	69	88.5	4355	70.62	63.12	160.381
County Sheriff	9	11.5	1812	29.38	201.33	114.807
All Agencies	78	100	6167	100	79.06	74.720

Examining Table 5.7, the 69 municipal law enforcement agencies comprise 88.5% of the agencies that reported receiving internet crime complaints in 2006. These 69 agencies received approximately 70% (n=4355) of the total internet crime complaints received, resulting in a mean of 63.12 internet crime complaints per agency. The county sheriff's departments comprised 11.5% of the agencies reporting at least one internet crime complaint in 2006, but received a share of the internet crime complaints that was disproportionately larger. The 9 county sheriff's departments in the responding sample received approximately 30% (n=1812) of the total number of internet crime complaints reported to local law enforcement agencies in 2006, with a mean of 201.33 internet crime complaints per agency. It is possible that with a larger sample this distinction, whether an agency is a county sheriff's agency or a municipal law enforcement agency will yield a statistically significant correlate of the number of internet crimes complaints received.

The Variety of Internet Crimes Reported to Police

This section of the chapter builds upon the above discussion of the number of internet crime complaints received by local agencies in 2006 by examining the various *types* of internet crimes reported to those agencies. This discussion examines the frequencies at which the various types of internet crimes are represented in the total number of internet crime complaints, as well as, the number of accurately counted complaints and the number of estimated complaints

reported by the agencies in the responding sample.

In Table 5.8, the total number of internet crime complaints received by the responding sample in 2006 is disaggregated into 20 different forms of internet crime[40]. It is interesting and somewhat surprising to note that all 20 forms of internet crime are represented among the 6167 internet crime complaints received by local law enforcement agencies in the responding sample. In other words, at least one instance of each form of internet crime was reported to the police during the 2006 calendar year.

A relatively small number of internet crime varieties accounted for a large proportion of the total number of internet crimes reported to local law enforcement agencies in the responding sample. The most commonly reported type of internet crime reported to police was misuse of a credit card (n=1249) followed closely by identity theft (n=1247), harassment via email and/or the internet (n=738), fraud via electronic funds transfer (n=580), criminal solicitation (n=529) and sexual solicitation of a minor (n=356). Together, these 6 types of internet crime account for over three-quarters (approximately 76.2%) of the total number of internet crime complaints received by local law enforcement agencies in the responding sample.

Several characteristics of the above crimes are worth noting. First, the most commonly reported internet crimes are among the more serious forms of internet crime. Such a finding is consistent with the existing literature concerning citizen reporting practices of traditional forms of crime. Citizens are more likely to report serious crimes (Walker and Katz, 2008). The nature of each of the most commonly reported crimes is very similar to their traditional crime counterparts; and, the investigation of each of these crimes would require little more technical expertise than their traditional counterparts. The least commonly reported internet crimes were

[40] Included in the 20 different forms of internet crime is an "other" category including any crimes not included on the survey questionnaire.

the dissemination of a computer virus (n=8) and launching a denial of service attack (n=4).

Table 5.8 Types of internet crime complaints received to local law enforcement agencies in 2006

	Total	Percent
Misusing a credit card*	1249	20.25
Identity theft*	1247	20.22
Harassment*	738	11.97
Fraud via electronic funds transfer*	580	9.4
Criminal solicitation*	529	8.58
Sexual solicitation of a minor*	356	5.77
Dissemination of SPAM email	283	4.59
Intimidation of another*	275	4.46
Pandering obscenity or pornography*	224	3.63
Distributing child pornography*	172	2.79
Stalking*	158	2.56
Accessing a computer without authorization	98	1.59
Other crime specified by the agency*	92	1.49
Inciting violence*	38	0.62
Interfering with a custody order*	37	0.6
Commission of a hate crime*	34	0.55
Making terroristic threats*	25	0.41
Inciting panic*	20	0.32
Dissemination of a computer virus*	8	0.13
Launching a denial of service attack	4	0.65
Total of all types	6167	**

*Agencies were asked to only include these crimes if they were committed via the internet and/or email.
**Total does not equal 100% due to rounding

C*omparing Accurate and Estimated Counts of Internet Crime Complaints*

Earlier in this chapter, a distinction was made between counts of internet crime complaints that were accurate counts and those that were estimates. The following section applies that distinction to the current discussion by examining whether the frequency with which the various forms of internet crime are reported to local law enforcement agencies in 2006 varies across types of internet crime counts—accurate counts or estimated counts. Table 5.9 presents the frequency with which each type of internet crime was reported to local law enforcement agencies in the responding sample based on accurate counts of complaints and Table 5.10 presents the same data for the estimated counts of internet crime complaints.

Table 5.9 Types of internet crimes (accurate) reported to local law enforcement agencies in 2006		
	Total	Percent
Identity theft*	279	20.36
Misusing a credit card*	260	18.98
Harassment*	155	11.31
Sexual solicitation of a minor*	118	8.61
Fraud via electronic funds transfer*	110	8.03
Intimidation of another*	102	7.45
Other crime specified by the agency*	72	5.26
Criminal solicitation*	71	5.18
Pandering obscenity or pornography*	62	4.53
Dissemination of SPAM email	36	2.63
Distributing child pornography*	33	2.41
Stalking*	20	1.46
Making terroristic threats*	20	1.46
Accessing a computer without authorization	15	1.09
Commission of a hate crime*	10	0.73
Inciting violence*	3	0.22
Launching a denial of service attack	2	0.15
Interfering with a custody order*	1	0.07
Dissemination of a computer virus*	1	0.07
Inciting panic*	0	0
Total of all types	1370	100
*Agencies were asked to only include these crimes if they were committed via the internet and/or email. **Total does not equal 100% due to rounding		

A comparison of Table 5.8, 5.9, Table 5.10, reveals that regardless of the type of count used—accurate, estimate or total—there is little change in terms of the rank ordering and the percentage of the total reported crimes for the most commonly reported types of internet crime. For the responding sample, regardless of the type of count used, complaints to police concerning identity theft and complaints involving the misuse of a credit card each account for roughly 20% of the overall number of complaints to local law enforcement agencies. Similarly, instances of harassment via email and/or the internet account for between 11% and 12% of the total number of internet crimes reported to police.

Table 5.10 Types of internet crimes (estimated) reported to local law enforcement agencies in 2006		
	Total	Percent
Misusing a credit card*	989	20.6
Identity theft*	968	20.2
Harassment*	583	12.15
Fraud via electronic funds transfer*	470	9.8
Criminal solicitation*	458	9.55
Dissemination of SPAM email	247	5.15
Sexual solicitation of a minor*	238	4.96
Intimidation of another*	173	3.6
Pandering obscenity or pornography*	162	3.38
Distributing child pornography*	139	2.9
Stalking*	138	2.88
Accessing a computer without authorization	83	1.73
Interfering with a custody order*	36	0.75
Inciting violence*	35	0.73
Commission of a hate crime*	24	0.5
Other crime specified by the agency*	20	0.42
Inciting panic*	20	0.42
Dissemination of a computer virus*	7	0.15
Making terroristic threats*	5	0.1
Launching a denial of service attack	2	0.04
Total of all types	4797	**
*Agencies were asked to only include these crimes if they were committed via the internet and/or email. **Total does not equal 100% due to rounding		

Section Summary

This section presented the findings concerning examinations of the volume and variety of internet crime complaints reported to local law enforcement agencies in the responding sample. Overall, nearly three-quarters of the agency representatives in the responding sample (including 78 of the 113 agencies completing the full questionnaire and 31 of the 37 agencies completing a short-version of the questionnaire) indicated that their agencies had received at least 1 complaint

concerning internet crime[41].

Of the 78 agencies completing the full-version of the survey questionnaire and reporting at least one internet crime complaint received during 2006, the number of complaints ranged from 1 complaint to 889 complaints, and the mean number of complaints received was 79.06. It should be noted that the range of the distribution is deceptive. As evidenced by both the absolute values of the mean ($\bar{x}$=79.06) and the median ($\tilde{x}$=21) as well as the position of each relative to the other[42], the distribution of the number of crime complaints received exhibited a positive skew. As such, over half of those agencies (n=41) received less than 25 complaints concerning internet crime.

Part II: The Actual Role of Local Police Agencies

As discussed in previous chapters, the preferred role of local law enforcement agencies in the sample is not synonymous with the role those agencies actually serve; furthermore, these two roles could be quite different. This section presents the findings from the current examination of the actual role local law enforcement agencies serve in regards to internet crime complaints.

The full-version of the survey questionnaire asked each agency representative to indicate in which of 26 different types of activities his or her agency engaged in response to internet crime complaints. Respondents were also permitted to indicate any activities in which their agencies engaged which did not appear on the questionnaire. The responses provided by each agency were used to examine the actual role local law enforcement agencies serve in controlling internet crime in two ways: through the individual crime control activities in which such

[41] A respondent completing the full-questionnaire was asked about internet crimes received during the 2006 calendar year only, whereas the shortened-version of the questionnaire asked the agency representative if his/her agency had *ever* received an internet crime complaint.

[42] In a symmetrical distribution the mean and median would be the same (Freund & Simon, 1992). In a distribution such as the present one in which the median value is less than the mean, the distribution exhibits a positive skew in that there is a concentration of cases in the lower end of the distribution (Freund & Simon, 1992).

agencies engage, and the total number of activities in which the various agencies in the responding sample engaged.

The Variety of Crime Control Activities of Local Law Enforcement Agencies

Table 5.11 presents the complete list of 26 crime control activities, as well as, the number and percentage of agencies in the responding sample that reported engaging in each activity. Of the twenty-five crime control activities included on the survey questionnaire, each was reportedly engaged in by at least one agency in the responding sample.

Table 5.11 Crime control activities engaged in by local law enforcement agencies

	Number (n=113)	Percent
1. Investigating complaints from citizens concerning internet crime	109	96.46
2. Investigating internet crime complaints referred by other agencies	90	79.65
3. Sharing information about internet crimes with other law enforcement agencies	83	73.45
4. Routinely collecting digital evidence during internet crime investigations	76	67.26
5. Distributing printed pamphlets/brochures about internet crime or internet safety	67	59.29
6. Having at least one part-time investigator assigned to investigate internet crimes	67	59.29
7. Having formally trained internet crime investigators	62	54.87
8. Conducting, or sponsoring, internet safety presentations	56	49.56
9. Providing links to websites about internet safety	31	27.43
10. Participating in an internet crime task force	30	26.55
11. Having at least one part-time investigator who specializes in internet crime	27	23.89
12. Conducting chat room stings for internet sex predators	26	23.01
13. Distinguishing between internet crime and traditional forms of crime	21	18.58
14. Having an internet crime unit	17	15.04
15. Maintaining membership in an internet security organization	15	13.27
16. Regularly monitoring online chat rooms	14	12.39
17. Conducting stings targeting distributors of child pornography	14	12.39
18. Distributing online pamphlets/brochures about internet crime or internet safety	13	11.15
19. Having at least one full-time investigator assigned to investigate internet crimes	13	11.15
20. Having at least one full-time investigator who specializes in internet crime	11	9.73
21. Maintaining a list of problematic websites and/or chat rooms	10	8.85
22. Providing links to websites with information on filtering programs	9	7.96
23. Providing an online means (e.g. online form) for reporting an internet crime or tip	9	7.96
24. Providing a phone number (other than 911) for reporting an internet crime or tip	8	7.08
25. Providing links to websites with information on anti-virus software	6	5.31
26. Any other effort, specified by the agency	2	1.77

Based on the findings presented in Table 5.11, it appears that the vast majority of local

law enforcement agencies, at least those in the responding sample, do indeed investigate internet crime complaints. In fact, the two most commonly reported crime control activities in which responding agencies engaged were investigating internet crime complaints from citizens and investigating internet crime complaints referred by other agencies.

Approximately 96.5% of the agencies (n=109) in the responding sample reported investigating complaints from citizens concerning internet crime; however, only about 79% of responding agencies reported engaging in investigations of internet crime complaints referred to them by other law enforcement agencies. While the vast majority of local law enforcement agencies in the responding sample were willing to investigate complaints of internet crime, it seems that a smaller portion of such agencies were willing to expend the effort to investigate such crimes, if the call was, or was *viewed* as, originating outside their jurisdictions.

The findings in Table 5.11 also indicate that law enforcement agencies in the responding sample are adapting to the challenges of investigating internet crime complaints. For example, over 67% of agency representatives in the responding sample indicated that investigators in their agencies routinely collect digital forms of evidence (e.g. hard drives, email, or saved files) as part of an internet crime investigation. This finding, if it generalizes to the population, indicates progress on behalf of law enforcement agencies in the collection of digital evidence during criminal investigations, in that a study by the FBI in 2005 found that less than 50% of agencies in their sample routinely collected digital forms of evidence during investigations.

It seems that despite a large portion (41 agencies, or approximately 36.27%) of the 113 agencies in the responding sample reported having neither a part-time nor a full-time investigator assigned to internet crime investigations, having at least one investigator assigned to investigate complaints concerning internet crime is more the norm than the exception Examining Table

5.12, just over half of the agencies in the responding sample reported having an investigator assigned to internet crime investigations on a part-time basis. Finally, only 13 of the agencies in the responding sample reported having an investigator assigned to internet crime investigations on a full-time basis. Five of these agencies had at least one full-time investigator, but eight of these agencies had both part-time and full-time internet crime investigators.

Table 5.12 Agency assignment of investigators to investigate internet crimes (n=113)

	Number	Percent
No investigator assigned to internet crime investigations	41	36.27
At least one part time investigator assigned to internet crime investigations	59	52.21
At least one full time investigator assigned to internet crime investigations	5	4.42
At least a full time *and* a part time investigator assigned to internet crime investigations	8	7.10
Total	113	100

Of the 113 agencies in the responding sample, 62 of the agencies (54.87%)[43] reported having at least one investigator who is formally trained—as opposed to being self-taught—to investigate internet crimes. Table 5.13 presents the resources agencies reported relying on for internet crime training. It is not surprising that the most commonly reported source of internet crime training, reported by over a third of the agencies in the responding sample was the state sponsored Ohio Peace Officer Training Academy (OPOTA). Approximately 30% of agencies reported relying on either a local expert or in-house training programs to train their internet crime investigators. The remaining agencies reported utilizing either private vendors/firms, a federal agency, another local agency, or a member of an internet crime task force.

Whereas the above findings suggest that having an investigator assigned to internet crime complaints is the norm for agencies in the responding sample, it does not appear that the same thing can be said concerning investigators specializing in internet crime investigations. Examining Table 5.14, a total of 33 agencies make use of an internet crime specialist. Of these

[43] This figure was drawn from line 7 of Table 5.13.

Table 5.13 Resources drawn upon for internet crime training (n=113)		
	Number	Percent of responding sample
Ohio Peace Officer Training Academy	38	33.63
In-house training or conducted by a local expert	34	30.09
Private vendor or private firm	22	19.47
Federal Agency	12	10.62
Another local agency	5	4.42
Internet crime task force personnel	4	3.54

agencies, 22 have at least one internet crime specialist assigned, on a part-time basis, to investigate internet crimes; 6 agencies have at least one internet crime specialist assigned on a full-time basis; and 5 agencies employ at least one full-time and one part-time investigator specializing in internet crime investigations. The vast majority of agencies (n=80) reported having no investigator specializing in internet crime investigations.

Table 5.14 Agency assignment of investigators specializing in internet crimes (n=113)		
	Number	Percent
No part-time or full-time internet crime specialists	80	70.80
At least one part-time internet crime specialist	22	19.47
At least one full-time internet crime specialist	6	5.31
Both full-time and part-time internet crime specialist	5	4.42

While the present study found that many agencies in the responding sample reported assigning investigators and specialists to internet crime investigations, only 15% of the agencies reported having a designated internet crime unit. This finding, however, may be a reflection of the characteristics of the agencies in the sample, as the majority of those agencies were smaller agencies. Such agencies could be expected to have fewer investigators and exhibit less of a need to assign their criminal investigators into units based on investigative specialization.

Despite the large percentage of respondents indicating that their agencies investigate internet crimes reported by citizens or referred by other law enforcement agencies, only 18.6% of

agencies in the responding sample indicated making a distinction between crimes committed via the internet and more traditional forms of crime for recordkeeping purposes. At first glimpse, a finding such as this may seem counter-intuitive when one considers the willingness of agencies to investigate internet crime complaints. However, this finding is easily explainable if one considers that neither the Uniform Crime Reports (UCR) nor the National Incident Based Reporting System (NIBRS) makes a distinction between the two types of crime.

Table 5.15 Agency Participation in Internet Crimes Task Forces (n=113)

	Number	Percent
No participation in internet crimes task force	79	69.9
Current participation & no past participation	4	3.5
Past participation & no current participation	3	2.7
Past & current participation	27	23.9

A number of local law enforcement agencies in the responding sample reported engaging in cooperative efforts to address internet crime complaints; however, some of these cooperative efforts were more popular among agencies than other such activities. Examining Table 5.15, approximately 27% of agencies in the responding sample participated in an internet crime task force (e.g. Crimes Against Children Task Force) at the time of completing the questionnaire. Table 5.16 presents further findings on participation in internet crime task forces for agencies in the responding sample. Of the 30 agencies participating in an internet crimes task force at the time of completing the survey, the vast majority of those agencies (n=27) indicated past participation with an internet crimes task force[44]. Furthermore, four additional agencies were not participating in any internet crimes task force at the time of completing the survey but had done so in the past. Overall, approximately 30% of agencies in the responding sample were involved

[44] From the data it is not known whether the agencies were continuously involved in the same task force or if the participation was intermittent. It is also not known whether a respondent's participation in the past and present involved participation in the same task force or in several different task forces.

in internet crimes task force either at the time of completing the survey or in the past.

The cooperative crime control activities in which local law enforcement agencies in the responding sample engaged were not limited to participation in internet crimes task forces. As shown in Table 5.18, approximately three-quarters (n=83) of the agencies in the responding sample reportedly shared information concerning internet crimes with other agencies; however participation in more formalized information sharing networks was limited to a much smaller number of agencies in the responding sample. Examining Table 5.17, only 13.3% of the agencies (n=15) in the responding sample reported they were members of a cooperative information sharing network, a finding that is similar to the findings of research conducted by the FBI (2005) that very few law enforcement agencies surveyed were members of such an organization.

Table 5.16 Agency Membership in Cooperative Information Sharing Networks (n=113)

	Number	Percent
Sharing information about internet crimes with other law enforcement agencies	83	73.45
No membership in networks	98	86.7
Member of any network listed below	15	13.3
Infragard	6	---
High Tech Criminal Investigations Association	12	---
Computer Security Institute	0	---
Information Systems Security Association	1	---
Information Systems Audit & Control Association	0	---
Member of more than one networks	4	3.5
Member of all networks	0	0

Among the agencies in the responding sample who were members of an information sharing network, 6 agencies were members of the FBI's Infragard Program, 12 agencies were members of the High Tech Criminal Investigations Association, and one agency was a member of the Information Systems Security Association. While four agencies in the responding sample were members of two organizations, no agencies reported being members of more than two of

these networks.

Several of the agencies in the responding sample reported using a number of techniques to help inform citizens and/or prevent internet crime from occurring in their jurisdictions. As shown in Table 5.17, well over half of the agencies in the responding sample reported distributing printed pamphlets about internet and/or internet safety and half of the agencies in the responding sample reportedly conduct or sponsor presentations about internet safety.

Table 5.17 Techniques used to inform citizens or prevent internet crime

	Number	Percent
Distributing printed pamphlets about internet crime and/or internet safety	67	59.29
Conducting or sponsoring presentations about internet safety	56	49.56
Providing links to websites with information about internet safety	31	27.43
Distributing online pamphlets about internet crime and/or internet safety	13	11.15
Providing links to websites with information about filtering programs	9	7.96
Providing links to websites with information about anti-virus software	6	5.31

It is interesting to note that the observed majority of agencies that reported engaging in the above forms of internet crime prevention did not extend to offering such resources in online, or electronic, formats. Only 11% of agencies reported distributing online versions of pamphlets concerning internet crime and/or internet safety tips; 27% of agencies reported providing citizens with links to information concerning internet safety; and, less than 8% of agencies provided citizens with links to either anti-virus software or internet filtering software.

A number of agencies in the responding sample reported using various investigative techniques for investigating internet crime complaints. As shown in Table 5.18, a number of agencies reported regularly monitoring problematic internet sites and chatrooms or maintaining a list of such internet addresses. However, by and large, the technique that agencies most commonly reported using to investigate internet crimes was the use of internet sting operations targeting online offenders. One-fourth of the agencies in the responding sample reported using

this technique to address one or more forms of internet crime. The vast majority (n=26) of the agencies engaged in online sting operations in attempts to apprehend online sexual predators targeting children. Online sting operations were also used by a number of agencies to apprehend distributors of child pornography (n=14), prostitutes who solicit online (n=2), and distributors of online distributors of illicit and/or illegal drugs (n=4).

Table 5.18 Techniques used to investigate internet crime complaints

	Number	Percent
Agencies reportedly using any form of online sting	29	25.66
Agencies conducting online stings in chat-rooms	26	23.01
Conducting online stings targeting distributors of child pornography	14	12.39
Conducting online stings targeting online drug sales	4	3.54
Conducting online stings targeting prostitutes	2	1.77
Regularly monitoring online chat-rooms	14	12.39
Maintaining a list of problematic websites and/or chat-rooms	10	8.85
Providing an online means (e.g. online form) for reporting internet crime	9	7.96
Providing a phone number (other than 911) for reporting internet crime	8	7.08

A much less commonly used technique for addressing and investigating internet crime complaints was the use of a cyber tipline. Only about 8% of agencies in the responding sample reported providing citizens with an online means of reporting an internet crime. Even fewer agencies reportedly provided a phone number—other than 911—for citizens to report an internet crime.

The Overall Activity Scale

Whereas the preceding section examined the variety of different types of activities and techniques local law enforcement used in addressing internet crime, this section examines the overall degree of activeness of the agencies in the responding sample in responding to internet crime complaints. A cumulative score, with possible values from 0 to 26 inclusive, was

calculated for each agency. An agency's score on this Overall Activity Scale[45] is equal to the number of crime control activities (listed in Table 5.11) in which that agency reportedly engages in efforts to address internet crime complaints in its jurisdiction. Table 5.19 presents the distribution of scores on the Overall Activity Scale for the agencies in the responding sample.

Although the maximum possible value of the Overall Activity Scale score was 26 points, none of the agencies in the responding sample received the maximum score. The activity scores for the 113 agencies in the current sample ranged from 0 to 22 points, with a median score of 7 points (sd=4.401). Given some of the findings presented earlier in this chapter (e.g. the large number of agencies in the responding sample that received no internet crime complaints in 2006), it is interesting to note that only one of the agencies in the responding sample received a score of 0 points.

As indicated by the measures of central tendency, the majority of agencies (55.7%) were fairly active in responding to internet crimes and internet crimes. Each of these agencies received a total activity score between 1 and 7 points. Approximately one-third of the agencies in the responding sample were moderately active in addressing internet crime. These agencies reported engaging in a variety of activities, specifically between 8 and 14 activities, in efforts to address internet crime and/or internet crime complaints. Finally, approximately one-tenth of the agencies in the responding sample received activity scores between 15 and 22 points. These eleven agencies were the most active agencies in the sample in terms of the number of different activities and/or techniques used to control internet crime.

[45] It is important to identify two limitations of the activity score as a measure of overall activeness of an agency. First, an agency's activity score is a measure of the number of different types of activities in which the agency engages; and, thus it is not a measure of the frequency of the individual activities. Second, due to the exploratory nature of the current research, no attempt was made to weight the values assigned to each activities, and thus each activity is assigned the same value. These are both concerns for future research and will be discussed in greater detail in a later section of this dissertation.

A test of internal consistency using Cronbach's alpha was performed to examine the extent to which the items in the Overall Activity Scale score are related to one another, thus representing a scale that does indeed measure an "underlying construct" (Hair et al., 1998, p. 118). The reliability analysis shows that for these 26 activities the value of alpha is high (α=.844) indicating a high degree of internal consistency among the items.

Table 5.19 Distribution of agency scores on the Overall Activity Scale

Overall Activity Score	Number of Agencies	Percent
0 activities reported	1	0.9
1 activity reported	2	1.8
2 activities reported	6	5.3
3 activities reported	5	4.4
4 activities reported	10	8.8
5 activities reported	16	14.2
6 activities reported	12	10.6
7 activities reported	12	10.6
8 activities reported	6	5.3
9 activities reported	8	7.1
10 activities reported	9	8.0
11 activities reported	8	7.1
12 activities reported	2	1.8
13 activities reported	4	3.5
14 activities reported	1	0.9
15 activities reported	2	1.8
16 activities reported	1	0.9
17 activities reported	3	2.7
18 activities reported	3	2.7
19 activities reported	1	0.9
20 activities reported	0	0
21 activities reported	0	0
22 activities reported	1	0.9
Total	113	100.0

Part III: Explaining Local Police Agencies' Scores on the Overall Activity Scale

Previous sections of this chapter examined the volume and variety of internet crimes reported to the local law enforcement agencies in the responding sample, the variety of activities

in which agencies engage in responding to internet crime and internet crime complaints, and the creation of an Overall Activity Scale. The current section presents the findings of an examination of the ability of various organizational factors, representing the allocation of personnel, the agency's structural characteristics and other variables thought to be relevant to the role of local police agencies to explain agencies' scores on the Overall Activity Scale.

Each of the local law enforcement agencies in the responding sample was assigned a score on the Overall Activity Scale. This score was equal to the total number of crime control activities in which a particular agency reportedly engaged. The present section of this chapter discusses the ability of organizational variables to explain the Overall Activity Scale scores.

A Contingency Theory approach to explaining the agency scores on the Overall Activity Scale would suggest that an agency's degree of activity in regards to internet crime would be explained primarily by the environmental demands (i.e. contingencies) placed on that agency. In the present study, these environmental demands are operationalized as the number of internet crime complaints an agency received by in 2006.

Bivariate regression analyses were conducted to determine the ability of the environmental demands (i.e. the number of internet crime complaints an agency received in 2006) to explain the level of activity local police agencies in terms of controlling internet crime (i.e. agency scores on the Overall Activity Scale). Three separate bivariate regression models were constructed. One used the total number of internet crime complaints received as the measure of demand placed on the agency. A second model used the estimated number of internet crime complaints received as the predictor variable. Finally, a third was constructed that attempted to predict OAS scores with the total number of accurately counted internet crime complaints received in 2006. Regardless of the measure used, the results of the bivariate

regression models were the same—the number of internet crime complaints received by an agency in 2006 was not a statistically significant predictor of agency scores on the Overall Activity Scale. Furthermore, the value of the adjusted R^2 suggests that in each of the three bivariate regression models the number of internet crime complaints received was able to explain less than 1% of the variation in agency scores on the OAS explained.

Table 5.20 Results of bivariate regression equations to explain scores on the OAS

	B	SE	Beta	T value	Sig	Adj R^2
Total Number of Internet Crime Complaints	.004	.003	.121	1.286	.201	.006
Accurate Number of Internet Crime Complaints	.007	.009	.075	.788	.433	-.003
Estimated Number of Internet Crime Complaints	.005	.004	.124	1.316	.191	.006
Number of All Crime Complaints	3.755	.000	.303	3.148	.002***	.083

* p≤ .10
** p≤ .05
*** p≤ .01

While it appears that the number of internet crime complaints received was not a significant predictor of agency scores on the Overall Activity Scale, the total number of *all* types of crime reported to an agency was a significant predictor of agency scores on the Overall Activity Scale. Examining Table 5.20, a simple regression model including the total number of all crime types reported to each agency as a predictor of agency scores on the OAS was statistically significant ($p < .01$). The value of the adjusted R^2 suggests that the model explains 8.3% of the variation in agency scores on the Overall Activity Scale.

The above findings raise concerns that variables other than the demand placed on agencies might better explain agency scores on the Overall Activity Scale. For example, perhaps variables reflecting organizational characteristics of the agencies would better explain an agency's score on the Overall Activity Scale. To examine this possibility, the bivariate correlations of agency scores on the OAS were examined.

Overall, eighteen measures of organizational characteristics were found to be statistically significant correlates of agency scores on the Overall Activity Scale. Table 5.21 presents the correlation coefficient for the metric independent variables and the Point Biserial coefficient for each of these relationships.

When size of the population served by an agency is converted to a series of dummy variables, four of the agency sizes are significant correlates of agency scores on the Overall Activity Scale. Local law enforcement agencies serving very small ($p < .01$) or small populations ($p < .05$) tend to receive lower scores on the OAS and thus are less active than agencies serving populations of other sizes. Conversely, as reflected by their tendency to receive high scores on the Overall Activity Scale, local law enforcement agencies serving large ($p < .10$) or very large populations ($p < .01$) tend to be more active than agencies serving populations of other sizes in terms of responding to internet crimes complaints.

Four measures of structural characteristics of agencies were found to be significant bivariate correlates of agency scores on the OAS. Both measures of agency size—the number of full-time sworn officers ($p < .01$) and the total number of employees ($p < .01$)—are significantly significant correlates of agency scores on the Overall Activity Scale. In both cases, larger agencies tend to receive higher scores reflecting a higher level of activity in combating internet crime. Vertical differentiation—organizational height—is a statistically significant correlate of

agency scores on the OAS. Agencies of medium height—those with between 4 and 6 ranks—tended to engage in a greater number of crime control activities and thus receive higher scores on the Overall Activity Scale ($p < .05$) than either short or tall agencies. A second measure of organizational height—the number of ranks in an agency—was not a significant correlate of agency scores on the Overall Activity Scale. Finally, the number of specialized units within an organization, a measure of functional differentiation, is a statistically significant bivariate level, positive correlate of agency scores on the Overall Activity Scale. Agencies with a greater number of specialized units engage in a greater number of the activities on the OAS ($p < .01$). The correlation between agency scores on the OAS and a second measure of functional differentiation—the proportion of officers who are assigned to specialized, non-patrol duties—was not statistically significant.

Several measures of the manner in which personnel are allocated within agencies were statistically significant correlates of OAS scores assigned to agencies. First, an agency's degree of civilianization was a significant correlate of agency OAS scores. Agencies with a higher civilianization tended to score higher on the OAS than agencies with lower degrees of civilianization ($p < .05$); however, the correlation between OAS scores and civilianization was only statistically significant when civilianization was measured as the ratio of the number of civilian employees to the total number of employees. Administrative intensity—the degree to which sworn officers are assigned to administrative positions—was a statistically significant bivariate correlate of agency scores on the Overall Activity Scale. Agencies with a higher degree of administrative intensity tended to score lower on the OAS. The correlation between agency scores on the OAS and administrative intensity was significant regardless of whether administrative intensity is measured as the ratio of the number of sworn officers assigned to

Table 5.21 Bivariate Correlations of Structural Variables and Overall Activity Scale Scores		
		Overall Activity Scale score
Very Small Population (0,1)	Point Biserial	-.262
	Significance (2-tailed)	.005***
	N	113
Small Population (0,1)	Point Biserial	-191
	Significance (2-tailed)	.042**
	N	113
Large Population (0,1)	Point Biserial	.165
	Significance (2-tailed)	.081*
	N	113
Very Large Population (0,1)	Point Biserial	.335
	Significance (2-tailed)	.000***
	N	113
Civilianization 2 (Ratio of the # of civilian employees to # of all employees)	Pearson Correlation	.219
	Significance (2-tailed)	.023**
	N	108
Span of Control 2 (Number of contacts between supervisor and officer on typical shift)	Pearson Correlation	.206
	Significance (2-tailed)	.052*
	N	90
Admin Concentration 1 (# of sworn assigned to administration/Total # of employees)	Pearson Correlation	-.269
	Significance (2-tailed)	.004***
	N	111
Admin Concentration 2 (# of sworn officers assigned to administration/Total # of sworn officers)	Pearson Correlation	-.265
	Significance (2-tailed)	.005***
	N	112
Size 1 (# of FT sworn officers)	Pearson Correlation	.308
	Significance (2-tailed)	.001***
	N	112
Size 2 (# of all employees)	Pearson Correlation	.319
	Significance (2-tailed)	.001***
	N	111
Functional Differentiation 1 (The # of specialized units)	Pearson Correlation	.326
	Significance (2-tailed)	.000***
	N	112
CALEA Certified (0,1)	Point Biserial	.222
	Significance (2-tailed)	.020**
	N	110
Percentage of Female Officers	Pearson Correlation	.213
	Significance (2-tailed)	.024**
	N	113
Suburban PD (0,1)	Point Biserial	.227
	Significance (2-tailed)	.017**
	N	111
Urban PD (0,1)	Point Biserial	.177
	Significance (2-tailed)	.062*
	N	111
College/University in Jurisdiction (0,1)	Point Biserial	.328
	Significance (2-tailed)	.000***
	N	111
Officers have Collective Bargaining (0,1)	Point Biserial	.395
	Significance (2-tailed)	.000***
	N	112
Medium Height (0,1) (4-6 ranks in agency)	Point Biserial	.227
	Significance (2-tailed)	.016**
	N	113
		* p≤ .10 ** p≤ .05 *** p≤ .01

administrative positions to the total number of employees ($p < .01$) or as the ratio of the number of sworn officers assigned to administrative positions to the number of sworn officers ($p < .01$). Finally, the number of encounters between an officer and his/her supervisor during a typical shift—a measure of the span of control in an agency—is a statistically significant correlate of agency scores on the Overall Activity Scale ($p < .10$). Agencies in which more contact between a supervisor and his/her officers is the norm tended to receive higher scores on the Overall Activity Scale. A second measure of the span of control in local police agencies—the ratio of the number of sworn officers to the number of sworn officers holding a rank of sergeant or higher—was not a significant correlate of OAS scores.

Examining Table 5.21, six other measures of local police agencies were statistically significant correlates of agency scores on the Overall Activity Scale. Agencies with a college or university within the jurisdiction ($p < .01$) tended to receive higher scores on the OAS scale. Likewise, the correlations for an agency receiving CALEA certification ($p < .05$) and agencies with higher percentages of female officers ($p < .05$) tended to be more responsive to internet crime. Local law enforcement agencies serving urban ($p < .10$) and suburban jurisdictions ($p < .05$) tended to receive higher scores on the Overall Activity Scale. Finally, agencies in which the officers have the capacity for collective bargaining ($p < .01$) tended to receive higher scores on the Overall Activity Scale.

Part IV: An Exploratory Multivariate Regression Model

Throughout much of this chapter, the Overall Activity Scale score, a measure of the degree of activity of each agency, was presented and discussed. This score was obtained by summing the number of crime control activities in which local law enforcement agencies engaged in efforts to address internet crime and internet crime complaints. While agency scores

on the Overall Activity Scale could have range between 0 and 26, no agency received a score higher than 22 on the Overall Activity Scale. The distribution of scores on the Overall Activity Scale had a mean score of 7.83, a median of 7 points and a standard deviation of 4.401.

In the bivariate tests discussed earlier in this chapter, the number of internet crimes received was unrelated to agency scores on the Overall Activity Scale and the six subscales of which it is composed. It is possible that the ability of the number of internet crime complaints received to explain variation in the dependent variable is being suppressed by the uncontrolled influence of the organizational variables. To explore this possibility, a multivariate regression analysis was conducted to examine the ability of the number of internet crime complaints received to explain variation in agency scores on the Overall Activity Scale while simultaneously controlling for the effects of the organizational characteristics. The variables selected for inclusion in the multivariate regression model were the same variables identified earlier in this chapter as significant bivariate correlates of agency scores on the Overall Activity Scale and are presented in Table 5.21.

Prior to conducting the regression analysis, it was necessary to first address an issue with the data. First, the bivariate correlation coefficients of each of the pairings of independent variables were examined for potential problems of multicollinearity and three problematic relationships were indeed identified. In each of the problematic relationships, the value of the correlation coefficient far exceeded the conventional .70 cutoff.

Two of these problematic relationships were fairly easy to correct. In both of these cases, multiple measures of the same variable—agency size and administrative concentration—were highly correlated with each other. To solve the problem posed by the high degree of inter-correlation between these measures, the model was respecified in such a way as to include only

one of the measures. In both of these cases, the measure which had the highest correlation coefficient in regards to the dependent variable was selected for inclusion in the multivariate model.

Table 5.22 Independent Variables Selected for Inclusion in the Multivariate Model	
Agency Size	Total number of employees
Size of Population Served	Very Small (0,1)
	Small (0,1)
	Large (0,1)
	Very Large (0,1)
Organizational Height	Medium Height (0,1)
Civilianization	Ratio of the number of civilians to the total number of employees
Span of Control	The number of contacts between and officer and his/her supervisor on a typical shift
Administrative Intensity	Proportion of sworn officers assigned to administrative duties
Control Variables	CALEA accredited agency (0,1)
	Percentage of sworn officers who are female
	Agency is Urban (0,1)
	Agency is Suburban (0,1)
	Presence of a college/university within agency's jurisdiction (0,1)
	Officers have access to collective bargaining (0,1)
	Total Number of Internet Crime Complaints Received in 2006

The remaining problematic relationship involved the extremely high degree of correlation between the measure of agency size and the number of specialized units in that agency (r=.940). The potential threat, in terms of multicollinearity, posed by this correlation was corrected by excluding the number of specialized units from the multivariate regression model. This decision to include size rather than the measure of functional differentiation was based primarily on the large amount of evidence in the policing literature that size is a major predictor of organizational

characteristics and practices (Maguire, 2003). Table 5.23 presents the final list of independent variables selected for inclusion in the multivariate analysis[46].

Results of the Multiple Regression Analysis

As discussed above, a multivariate regression analysis was conducted to examine the degree to which variation in agency scores on the Overall Activity Scale is explained by the number of internet crime complaints received, while simultaneously controlling for the effects of the organizational characteristics a multivariate regression model was constructed. The results of that analysis are discussed here.

Table 5.23 Results of the Multivariate Regression Model ANOVA

	Sum of Squares	df	Mean Square	F	Sig
Regression	603.605	14	43.115	3.014	.001
Residual	1244.473	87	14.304		
Total	1848.078	101			

The multivariate model included thirteen measures of organizational characteristics and the number of internet crime complaints received as predictors of agency scores on the Overall Activity Scale. Examining Table 5.25, the results of this multivariate regression model indicated that the value of the F statistic for the model was indeed statistically significant ($p < .001$). Furthermore, as presented in Table 5.24, the model's coefficient of determination indicated that roughly one-third of the variation in the dependent variable was explained by the multiple regression model (R^2=.336). However, the proportion of the variation in agency scores on the Overall Activity Scale that is explained by the model is reduced substantially when the value of the adjusted coefficient of determination (adjusted R^2=.247) is examined. Using this more

[46] When a choice was made between two measures of the same organizational characteristic, the measure exhibiting the highest degree of correlation with the dependent variable—the agency scores on the Overall Activity Scale—was selected for inclusion in the regression model.

conservative measure[47] of the model's explanatory power, the analysis indicates that the independent variable and the twelve control variables explains about one-fourth of the variation in agency scores on the Overall Activity Scale (Hair et al., 2005).

Table 5.24 Model Summary for the Multivariate Model

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.571	.327	.218	3.78210

The multivariate model produced some troubling findings. Despite the statistical significance of the model's F-ratio, very few of the variables were significant. Examining Table 5.25, only the model's constant and the two of the dummy variable for suburban agencies reached the level of statistical significance.

Considering that the independent variables were included in the analysis because of their bivariate relationship with agency scores on the Overall Activity Scale, it seems especially troubling that *only* the dummy variable reflecting that an agency is a suburban department would be statistically significant. These findings raise the possibility that additional instances of multicollinearity exist between the control variables and are influencing the results of the regression analysis. However, the fact that the model flagged the dummy variable for suburban agencies as significant raises another possible explanation. It may very well be that agency characteristics have little to do with the activity levels of local police agencies and that a better explanation might be found by examining the characteristics of the jurisdiction being policing. Irregardless of the underlying cause, the only variable that emerged as significant predictor of an agency's score on the Overall Activity Scale was a dummy variable designation flagging a suburban law enforcement agency.

[47] The adjusted R^2 is used to compensate for inflation in the coefficient of determination due to number of Independent variables included in the model relative to the number of cases in the sample (Hair et al., 2005, p. 182). Considering the small number of cases in the responding sample for the present study, this measure of explained variation is especially appropriate for interpreting the various regression models.

The next chapter presents the author's conclusions and discussion of the findings. First, a discussion of the major findings is presented. Second, the limitations of the present study are discussed. Finally, several recommendations are made regarding future research efforts in the area of the role of local law enforcement in the age of the internet.

Table 5.25 Coefficients for the Multivariate Model

	Unstandardized Coefficients		Standardized Coefficients			95.0% Confidence Interval for B	
	B	Std. Error	Beta	t	Sig.	Lower Bound	Upper Bound
(Constant)	6.163	1.949		3.162	.002	2.289	10.037
Very Small Population (0,1)	-1.841	1.968	-.168	-.936	.352	-5.754	2.071
Small Population (0,1)	-.384	1.832	-.036	-.209	.835	-4.025	3.257
Large Population (0,1)	1.502	1.193	.145	1.259	.212	-.870	3.873
Very Large Population (0,1)	1.154	1.468	.108	.786	.434	-1.764	4.072
Civilianization	2.652	2.512	.111	1.056	.294	-2.341	7.645
Administrative Intensity	-4.550	5.434	-.088	-.837	.405	-15.351	6.252
Number of employees	.002	.002	.154	1.383	.170	-.001	.006
CALEA certified agency (0,1)	1.360	1.079	.131	1.261	.211	-.784	3.505
Percentage of female officers	.030	.060	.054	.507	.613	-.089	.150
PD is urban	1.075	1.222	.109	.880	.381	-1.354	3.503
PD is suburban	2.277	1.112	.264	2.047	.044	.066	4.487
College in Jurisdiction	1.288	1.001	.145	1.287	.201	-.701	3.277
Collective bargaining	-1.119	1.811	-.125	-.618	.538	-4.718	2.481
All net crimes reported	-.002	.003	-.061	-.599	.551	-.008	.004

Chapter Six: Summary and Conclusions

This chapter serves three purposes. First, the major findings presented in the previous chapter are presented and discussed. Second, the limitations of the present research are discussed. Finally, the author's suggestions for future research are discussed.

Major Findings

This section summarizes and discusses the major findings presented in the previous chapter. The discussion is organized in the following manner. First, the major findings concerning the preferred role of local police agencies are discussed. Second, the major findings concerning the enacted role of local law enforcement agencies are presented. Finally, the major findings concerning the ability of a contingency theory framework to explain the actual role of the police are discussed.

The Preferred Role of Local Law Enforcement Agencies Regarding Internet Crime

For the most part, internet crime does appear to be a problem that the citizenry places within the bailiwick of their local law enforcement officials. Nearly 70% (n=78) of the 113 agencies in the responding sample reportedly received at least one internet crime complaint during the 2006 calendar year. Furthermore, representatives from another 31 of 37 agencies completing a shortened version of the survey questionnaire reported receiving at least one internet crime complaint at some point in the past. Overall, nearly three-fourths of the 150 agencies in the responding sample had received an internet crime complaint at some point in the past.

Agencies, when asked, are able to provide counts of the number of internet crime complaints received. In the present study, agencies were asked to provide an accurate count of the number of complaints received during 2006 concerning twenty different types of internet

crime. If an accurate count was not available, the agency representative was asked to provide an estimate of the number of such complaints received during 2006. Overall, the 78 agencies in the responding sample reported receiving a total of 6167 internet crime complaints (including 1370 accurately counted complaints and an estimated 4797 complaints). The number of reports received by individual agencies ranged from a low of 1 complaint to a high of 889 complaints, with a mean of 79.06 complaints per agency[48]. However, the mean is rather misleading as an indicator of central tendency for the present data as half of the agencies received 21 or fewer such complaints.

Five specific internet crimes account for over 60% of the total number of internet crime complaints received by local law enforcement agencies in the present sample. These crimes include the misuse of a credit card (n=1249), identity theft (n=1247), harassment (n=738), fraud via electronic funds transfer (n=580) and criminal solicitation via the internet and/or email (n=529). Regardless of whether one examines the total number of complaints, the accurate counts of complaints or the estimated counts of complaints, these five crimes remain the most commonly reported internet crimes.

The five most commonly reported internet crimes share two characteristics. First, each is among the more serious forms of internet crime, in that each has a high potential for personal loss (either monetary loss or personal injury). This finding is consistent with what is known about reporting practices of traditional forms of crime. Citizens are more likely to report serious crime (Walker and Katz, 2008). Second, each of the five most common internet crimes reported is very similar to a traditional form of crime and the investigation of each would require little more technical expertise than the more traditional forms of crime. It is interesting to note that

[48] The mean value is calculated based on the number of agencies receiving at least one complaint during 2006.

the least commonly reported crimes—dissemination of a computer virus (n=8) and launching of a denial of service attack (n=4)—would require a high level of technical expertise to investigate.

The Enacted Role of Local Law Enforcement Agencies Regarding Internet Crime

In the present study representatives from local law enforcement agencies in Ohio were asked to indicate in which of 26 different types of crime control activities[49] their agencies engaged in response to internet crime complaints. Each of the 25 types of crime control activities was engaged in by at least one agency in the responding sample.

The crime control activities in which agencies most commonly engaged include: investigating internet crimes reported by citizens in the jurisdiction (96.46%), investigating internet crimes referred to them by other law enforcement agencies (79.65%), sharing information about internet crimes with other law enforcement agencies (73.45%), routinely collecting digital evidence during internet crime investigations (67.26%), distributing printed pamphlets/brochures about internet crime or internet crime safety (59.29%) and having at least one part-time investigator to investigate internet crimes (59.29%). These findings support the assertion that local law enforcement agencies in the responding sample are responding, either through investigation and/or prevention, to citizen complaints regarding internet crime.

The number of activities in which each agency reportedly engaging was summed and an additive index, the Overall Activity Scale, was created. This scale had a relatively high level of internal reliability (α=0.844)[50] suggesting that it does indeed measure some underlying construct. Scores on the Overall Activity Scale ranged from a low score of 0 to a high score of 22, with 56.6% of agencies receiving a score of 7 or less. It is interesting to note that only *one* of the 113 agencies in the responding sample reported engaging in none of the 26 activities.

[49] Including an "other" category for respondents to indicate any crime control activity not included on the list.
[50] Later elimination of six items increased this measure of internal reliability to 0.860).

Explaining the Enacted Role of Law Enforcement Agencies with Contingency Theory

Contingency theorists argue that organizational behavior is largely explained by environmental factors (contingencies) that exert an influence on the organization. The present study, by examining the ability of a contingency in the organizational environment of local law enforcement agencies (the number of internet crime complaints received) to explain the agency's score on the Overall Activity Scale, represents a test of this most basic of tenets of the contingency theory framework of organizational behavior.

The findings of the present study are largely unsupportive of a contingency theory approach to explaining the response of law enforcement agencies to internet crime complaints. The results of a simple regression analysis revealed that the number of internet crime complaints only explains about 2% of the variation in agency scores on the Overall Activity Scale. In fact, the present study found that the number of all crimes reported to an agency was a much better predictor of agency scores on the Overall Activity Scores. The total number of crimes reported to an agency explained 10% of the variation in agency scores on the Overall Activity Scale.

A multivariate regression model was conducted to examine the possibility that the influence of the contingency variable was being suppressed by one or more of the organizational characteristics of police agencies. Measures of ten organizational characteristics were used as control variables in a multivariate regression model with the number of internet crime complaints received as the dependent variable and agency scores on the Overall Activity Scale as the dependent variable; however, complications due to multicollinearity between the organizational characteristics produced indecipherable results. One variable did come to the forefront as a significant predictor of the number of activities in which local law enforcement agencies engaged—agencies in suburban areas tended to engage in a greater number of crime control

activities than did their urban and rural counterparts. This finding hints at a possible explanation. Perhaps it is not the characteristics of the agency, but is instead the jurisdiction being policed that explains the activities of local law enforcement agencies. While the current study does not provide a definitive answer to the question of which variables explain the activities of local law enforcement agencies in responding to internet crime complaints, the study does provide an answer to the question of which variable does not explain agency responses. One answer is that citizen demands operationalized as the number of internet crime complaints an agency receives does *not* explain the variety of activities in which agencies engage in an effort to combat internet crime.

Limitations of the Current Research

The present study has presented a number of findings that represent an important first step in examining an understudied area in the existing literature by examining the both preferred and actual roles of local law enforcement agencies in controlling internet crime. While this research adds to our understanding of the role of the police in regards to a still developing area of crime, there are several limitations to the current study.

First, the most substantial limitation is posed by the small sample of agencies from which the data were drawn. Despite a number of efforts to collect data from all 871 police municipal police departments in the state of Ohio, the response rate for the current study was approximately 17%. While this rate is comparable to many of the empirical studies of internet crime in the existing literature, it limits the author's ability to generalize the findings beyond the present sample. A larger sample size would enhance the ability to generalize beyond the sample studied, but would also allow for the use of more sophisticated techniques of statistical analysis.

A second limitation of the present research is that all of the data was collected from law

enforcement agencies within the state of Ohio. While King (2008) provides evidence that Ohio is very representative of the United States, limiting the current study to agencies in one state eliminated any variation in legal definitions of internet crime across state lines. While eliminating this variation allowed the author to examine the activities of a group of local law enforcement agencies that were all operating with largely the same legal definitions of internet crimes, it limits the author's ability to generalize beyond the sample studied and to examine the prescribed role of local law enforcement agencies.

Third, the measure of the overall activity level of local law enforcement agencies was actually more of a measure of the variety of activities. This measure of the overall activity of an agency did not allow the author to examine the frequency with which agencies engaged in activities or which activities agencies engaged weighted by the amount of resources required for each activity.

Finally, the analysis of a multivariate regression model examining the ability of the number of internet crime complaints to explain agency scores on the Overall Activity Scale while controlling for the effects of the organizational characteristics of local law enforcement agencies was hindered by issues of multicollinearity. While few of the measures of organizational characteristics were highly correlated with one another at the bivariate level, issues of multicollinearity were present and contributed to initial findings that were largely indecipherable.

Future Research

The line of research begun here is worth continuing and devoting future research efforts to pursuing. However, future research endeavors should strive to maximize response rates and obtain the largest sample possible. Such conditions are prerequisites for conducting

sophisticated statistical analyses. A major obstacle to be addressed will be identifying the reasons that local law enforcement agencies are reluctant to complete surveys such as the one used to collect the data for use in the present study and find ways to overcome such reluctance and gain the necessary cooperation.

Future research efforts should continue to explore the demands placed on local law enforcement agencies in regards to internet crime complaints by examining the motivations of citizens who report such crimes to the police. For example, does a citizen report an internet crime in hopes that the police will identify the offender or does the citizen report such crimes simply to placate the insurance company?

Furthermore, future research should strive to identify solutions to the problems of multicollinearity such as those encountered in the present study. Such solutions will prove necessary if researchers are to conduct multivariate analyses that incorporate appropriate controls for organizational characteristics and still yield interpretable results.

Finally, future research should continue to examine the concept of police activeness in controlling internet crime. The measure used here was an overall measure of activity. Future research should continue this line of research by examining activity in terms of the frequency with which activities are engaged in and by possibly weighting the activities by the amount of resources that each requires.

Appendix A

Table of Descriptive Statistics for the Independent Variables

Table A1 Descriptive Statistics for the Independent Variables

	N	Minimum	Maximum	Mean	Std Dev
Civilianization 1 (# ft civilian/# ft sworn officers)	113	.00	2.24	.2141	.32669
Civilianization 2 (# civilian/# employees)	113	.00	1.31	.1660	.17636
Patrol Concentration 1 (# patrol/# sworn officers)	113	.00	1.33	.5352	.30629
Patrol Concentration 2 (# patrol/# ft sworn officers)	113	.00	4.00	.7101	.52068
Span of Control 1 (# patrol/# sgt or above)	113	.00	9.00	2.3921	1.7002
Span of Control 2 (# contacts with supervisor)	113	0	35	3.47	4.851
Administrative Concentration 1 (# admin/# employees)	113	.00	.50	.1005	.09309
Administrative Concentration 2 (# admin/# sworn officers)	113	.00	.50	.1195	.09951
Size 1 (# ft sworn officers)	113	0	1878	66.17	214.837
Size 2 (# employees, ft and pt)	113	0	2252	88.89	261.443
Age 1 (Decade in which agency created)	113	0	1990	--	813.229
Age 2 (Era in which agency is created) (1=pre-1900, 2=1900-1949, 3=post-1950)	113	0	3	--	1.067
Vertical Differentiation 1 (# of Ranks)	113	0	8	3.97	1.436
Vertical Differentiation 2 (1-3, 4-6, 7+ ranks)	113	0	3	--	.541
Spatial Differentiation	113	0	1992	36.32	192.804
Functional Differentiation 1 (# specialized units)	113	0	79	3.77	8.673
Functional Differentiation 2 (# nonpatrol/# ftsworn officers)	113	-3.00	1.00	.1837	.46336
Percentage of officers who are minority	113	.00	50.00	4.5177	9.5722
Percentage of officers who are female	113	.00	55.00	5.6035	7.6249
Percentage of budget spent on non-salary exp.	113	.00	85.00	19.1214	16.7205
Percentage of local/county budget	113	.00	65.00	18.7751	15.7896
CALEA certified agency	113	0 87%	1 23%	--	---
Local agency	113	0 10.6%	1 89.4%	--	---
Urban Department	111	0 76.6%	1 23.4%	--	---
College/university in jurisdiction	113	0 64.6	1 33.6%	--	---
NIBRS compliant agency	113	0 29.6%	1 70.4%	--	---
Officers have collective bargaining	113	0 33.9%	1 66.1%	--	---

Appendix B

Tables of Correlation Matrices of Independent Variables

Table B1 Correlations between the Personnel Variables and All Independent Variables								
	Civil 1	Civil 2	Patrol 1	Patrol 2	Span 1	Span 2	Admin 1	Admin 2
Civil1	1	.812	.078	-.056	.099	.134	-.163	-.076
Civil2	.812	1	.152	-.025	.142	.135	-.127	-.044
Patrol1	.078	.152	1	.596	.508	.160	.267	.341
Patrol2	-.056	-.025	.596	1	.364	.000	.374	.390
Span1	.099	.142	.508	.364	1	.085	-.036	-.001
Span2	.134	.135	.160	.000	.085	1	-.136	-.112
Admin1	-.163	-.127	.267	.374	-.036	-.136	1	.963
Admin2	-.076	-.044	.341	.390	-.001	-.112	.963	1
Size1	.034	.045	.078	-.048	.135	.011	-.051	-.038
Size2	.069	.065	.080	-.048	.148	.012	-.061	-.044
Age1	.089	.102	.247	.196	.123	.049	.063	.053
Age2	-.056	-.030	.184	.187	-.001	-.001	.126	.100
Height1	.505	.313	.086	-.036	.177	.066	-.117	-.059
Height2	.348	.387	.187	-.141	.178	.159	-.194	-.106
Spatial	.037	.052	.078	-.007	.104	-.024	-.044	-.035
Function	.050	.055	.099	-.056	.170	.060	-.086	-.061
Function2	.188	.209	-.318	-.808	-.083	.034	-.230	-.219
CALEA	-.023	.008	.059	.028	-.002	-.072	-.138	-.146
Minority	-.029	-.041	.210	.241	.037	.076	.012	.038
Female	.055	.050	-.068	-.170	.040	-.053	-.128	-.118
Nonsalary	-.103	-.132	.030	-.005	.005	-.187	.204	.145
Budgetshare	.002	.013	.209	.036	.071	-.025	.153	.120
Localcounty	.499	.369	-.063	-.134	.071	-.036	-.182	-.110
Urban	.102	.032	-.128	-.018	-.373	-.224	.120	.117
College	.182	.160	.091	-.047	.204	.115	-.206	-.186
NIBRS	.097	.078	-.107	-.077	-.118	-.079	.023	.000
Collective	.337	.393	.337	-.137	.333	.333	-.379	-.260

Table B2 Correlations between the Personnel Variables and All Independent Variables									
	size1	size2	age1	age2	height1	height2	spatial	function1	function2
Civil1	.034	.069	.089	-.056	.505	.348	.037	.050	.188
Civil2	.045	.065	.102	-.030	.313	.387	.052	.055	.209
Patrol1	.078	.080	.247	.184	.086	.187	.078	.099	-.318
Patrol2	-.048	-.048	.196	.187	-.036	-.141	-.007	-.056	-.808
Span1	.135	.148	.123	-.001	.177	.178	.104	.170	-.083
Span2	.011	.012	.049	-.001	.066	.159	-.024	.060	.034
Admin1	-.051	-.061	.063	.126	-.117	-.194	-.044	-.086	-.230
Admin2	-.038	-.044	.053	.100	-.059	-.106	-.035	-.061	-.219
Size1	1	.997	.102	-.080	.090	.258	.251	.944	.119
Size2	.997	1	.109	-.085	.138	.278	.248	.940	.122
Age1	.102	.109	1	.784	.061	-.029	.085	.086	-.128
Age2	-.080	-.085	.784	1	-.043	-.039	.120	-.058	-.174
Height1	.090	.138	.061	-.043	1	.420	.023	.095	.112
Height2	.258	.278	-.029	-.039	.420	1	.098	.252	.346
Spatial	.251	.248	.085	.120	.023	.098	1	.232	.045
Function	.944	.940	.086	-.058	.095	.252	.232	1	.123
Function2	.119	.122	-.128	-.174	.112	.346	.045	.123	1
CALEA	.305	.299	.233	.195	-.032	.135	.045	.316	-.010
Minority	.415	.420	.072	-.027	.035	.081	.045	.383	-.217
Female	.366	.373	.007	-.155	.096	.256	.045	.381	.215
Nonsalary	-.110	-.112	.007	-.010	-.163	-.361	.045	-.170	-.039
Budgetshare	.179	.176	.165	.040	-.078	-.108	.045	.145	.093
Localcounty	.041	.079	-.033	-.216	.323	.321	.045	.036	.230
Urban	-.270	-.267	-.062	.065	.027	-.241	.045	-.291	-.100
College	.325	.344	.158	-.067	.204	.385	.045	.305	.177
NIBRS	.047	.054	-.092	-.171	.055	-.148	.045	.016	.007
Collective	.210	.220	.056	-.066	.225	.552	.045	.257	.350

Table B3 Correlations between the Personnel Variables and All Independent Variables

	CALEA	Minority	Female	Nonsalary	Budget share	Local/county	Urban	College	NIBRS	Collective B
Civil1	-.023	-.029	.055	-.103	.002	.499	.102	.182	.097	.337
Civil2	.008	-.041	.050	-.132	.013	.369	.032	.160	.078	.393
Patrol1	.059	.210	-.068	.030	.209	-.063	-.128	.091	-.107	.337
Patrol2	.028	.241	-.170	-.005	.036	-.134	-.018	-.047	-.077	-.137
Span1	-.002	.037	.040	.005	.071	.071	-.373	.204	-.118	.333
Span2	-.072	.076	-.053	-.187	-.025	-.036	-.224	.115	-.079	.333
Admin1	-.138	.012	-.128	.204	.153	-.182	.120	-.206	.023	-.379
Admin2	-.146	.038	-.118	.145	.120	-.110	.117	-.186	.000	-.260
Size1	.305	.415	.366	-.110	.179	.041	-.270	.325	.047	.210
Size2	.299	.420	.373	-.112	.176	.079	-.267	.344	.054	.220
Age1	.233	.072	.007	.007	.165	-.033	-.062	.158	-.092	.056
Age2	.195	-.027	-.155	-.010	.040	-.216	.065	-.067	-.171	-.066
Height1	-.032	.035	.096	-.163	-.078	.323	.027	.204	.055	.225
Height2	.135	.081	.256	-.361	-.108	.321	-.241	.385	-.148	.552
Spatial	.034	.038	.013	-.107	.226	-.028	-.074	.014	-.119	.120
Function	.316	.383	.381	-.170	.145	.036	-.291	.305	.016	.257
Function2	-.010	-.217	.215	-.039	.093	.230	-.100	.177	.007	.350
CALEA	1	.138	.111	-.252	-.097	-.103	-.188	.152	-.116	.090
Minority	.138	1	.421	-.154	.128	-.047	-.152	.285	-.076	.017
Female	.111	.421	1	-.094	.114	.238	-.196	.329	.093	.241
Nonsalary	-.252	-.154	-.094	1	.316	-.075	.161	-.131	.049	-.175
Budgetshare	-.097	.128	.114	.316	1	.013	-.019	.069	.033	.088
Local	-.103	-.047	.238	-.075	.013	1	.109	.302	.179	.250
Urban Agency	-.188	-.152	-.196	.161	-.019	.109	1	-.329	.046	-.393
College	.152	.285	.329	-.131	.069	.302	-.329	1	.058	.359
NIBRS	-.116	-.076	.093	.049	.033	.179	.046	.058	1	-.031
Collective B	.090	.017	.241	-.175	.088	.250	-.393	.359	-.031	1

REFERENCES

Abbate, J. 1999. Inventing the Internet. Cambridge, MA: MIT

Applegate, B.K. 1997. Specifying Public Support for Rehabilitation: A Factorial Survey Approach. Doctoral Dissertation, University of Cincinnati, Division of Criminal Justice. Cited in King, W.R. 2009. "Organizational Failure and the Disbanding of Local Police Agencies." *Crime & Delinquency*, OnlineFirst: Available online at http://cad.sagepub.com/content/early/2009/09/08/0011128709344675.

Barlow, D.E. and M.H. Barlow. 1999. "A political economy of community policing." *Policing: An International Journal of Police Strategies & Management*, Vol. 22, Issue 4: 646-74.

Bennett, G. 1987. Crime Warps: The future of crime in America. Garden City, NY: Anchor Books.

Berners-Lee, T. 1996. "The Web: Past, present and future." World Wide Web Consortium. Available online: http://www.w3.org/People/Berners-Lee/1996/ppf.html.

Bequai, A. 1978. White Collar Crime: A 20th century crisis. Lexington, MA: Lexington.

Bittner, E. 1970. "The Functions of Police in America", in Brandl and Barlow (eds.). 2004. The Police in America: Classic and contemporary readings. Belmont, CA: Wadsworth.

Brenner, S. 2003. "State Cybercrime Laws: A survey." *University of Richmond Journal of Law and Technology*, Vol. 7, Issue 3.

Burns, T. and G.M. Stalker. 1961. The Management of Innovation. New York: Oxford.

Burton Jr., V.S., J. Frank, R.H. Langworthy and T.A. Barker. (1993). "The prescribed roles of Police in a Free Society: Analyzing state legal codes" *Justice Quarterly*, Vol. 10, Issue 4: 683-695.

Capeller, W. 2001. "Not Such a Neat Net: Some comments on virtual criminality." *Social and Legal Studies,* Vol. 10, Issue 2: 229-242.

Castells, M. 1985. "High Technology, Economic Restructuring and the Urban-regional Process in the United States." in M. Castells (ed.). High Technology, Space and Society*, Urban Affairs Annual Review*, Vol. 28. Beverly Hills, CA: Sage.

Castells, M. 2001. The Internet Galaxy: Reflections on the Internet, Business, and Society. New York: Oxford University Press

Chatterjee, B.B. 2001. "Last of the Rainmacs? Thinking about pornography in cyberspace." in D.S. Wall (ed.). Crime and the Internet. London: Routledge

Chawki, M. 2006. "Anonymity in Cyberspace: Finding the balance." Computer Crime Research Center. Available online: http://www.crime-research.org/articles/2110.

Conseil Européen pour la Recherche Nucléaire. 2007. "What is CERN?" Available online: http://press.web.cern.ch/public/content/Chapters/AboutCERN/WhatIsCERN/CERNName/CERNName-en.html.

Crank, J.P. 1990. "The influence of environmental and organizational factors on police style in urban and rural environments." *Journal of Crime and Delinquency*, Vol. 27, Issue 2: 166-189.

Crank, J.P. and L.E. Wells. 1991. "The Effects of Size and Urbanism on Structure Among Illinois Police Departments." *Justice Quarterly*, Vol. 8, Issue 2: 170-185.

Donaldson, L. 1985. In defence [sic] of Organizational Theory: a reply to the critics. New York: Cambridge University Press.

Donaldson, L. 1996. The Normal Science of Structural Contingency Theory. London: Sage.

D'Ovidio, R., and J. Doyle. 2003. "A Study on Cyberstalking: Understanding investigative hurdles." *FBI Law Enforcement Bulletin*, Vol. 72, Issue 3: 10-17.

Eck, J.E. and W. Spelman. 1987. "Who Ya Gonna Call? The Police as Problem-busters." *Crime and Delinquency*, Vol. 33, Issue 1: 31-52.

Federal Bureau of Investigation. 2005. "2005 FBI Computer Crime Survey." Washington, DC: Federal Bureau of Investigations. Available online: http://www.fbi.gov/publications/ccs2005.pdf.

Federal Bureau of Investigation. 2005a. "Results of the FBI Pittsburgh Division 2005 Cyber Crime Survey." Washington, DC: Federal Bureau of Investigations.

Federal Trade Commission. 2003. "Federal Trade Commission—Identity Theft Survey Report." Available online: http://www.ftc.gov/os/2003/09/synovatereport.pdf.

Felson, M. 2002. Crime in Everyday Life. (3rd ed.). Beverly Hills, CA: Sage.

Ferraro, M.M., and R.L. Hammer. 2006. "Computer-assisted and internet crime." in R.L. Hammer, B. Moynihan and E.M. Pagliaro. eds. 2006. Forensic Nursing: A handbook for practice. Sudbury, MA: Jones and Bartlett.

Finkelhor, D., K.J. Mitchell, and J. Wolak, 2005. "Online victimization: What youth tell us." in S.W. Cooper, R.J. Estes, A.P. Giardino, N.D. Kellogg, and V.I. Vieth. eds. Medical, legal, and social science aspects of child sexual exploitation: A comprehensive review of pornography, prostitution, and Internet crimes, Vol. 1. St. Louis, MO: G. W. Medical.

Fischer, C.S. 1985. "Studying Technology and Social Life" in M. Castells (ed.). High Technology, Space and Society, *Urban Affairs Annual Review*, Vol. 28. Beverly Hills, CA: Sage.

Fisher, B.S., F.T. Cullen and M.G. Turner. (2002). "Being Pursued: Stalking victimization in a National Study of College Women" Criminology and Public Policy, Vol. 1, Vol. 2: 257-308.

Franklin, C.J. 2006. The investigator's guide to computer crime. Springfield, IL: Charles C. Thomas.

Fox, S. 2005. "Online Threats and Fears are Changing Consumer Behavior." Presentation at the IAPP Privacy Academy 2005 in Las Vegas, NV.

Fox, S. 2006. "Internet Usage Trends—Through the Demographic Lens." Pew Internet and American Life Project. Available online: http://www.pewinternet.org/ppt/Fox_FTC_Nov_6_%202006.pdf.

Friedrichs, D.O. 2004. Trusted Criminals: White collar crime in contemporary society. (2nd ed.). Belmont, CA: Wadsworth.

Gardner, W.D. 2007. "Online Shopping Report: Sales Up 24% In 2006." *Information Week*, January 4, 2007. Available online: http://www.informationweek.com/story/showArticle.jhtml?articleID=196801126.

Goldstein, H. 1979. "Improving Policing: A problem oriented policing approach." *Crime and Delinquency*, Vol. 25, Issue 2: 236-258.

Goodman, M. 2001. "Making Computer Crimes Count." *FBI Law Enforcement Bulletin*, Vol. 70, Issue 8: 10-17.

Goodman, M. 1997. "Why the Police Don't Care About Computer Crime." *Harvard Journal of Law and Technology*, Vol. 10, Issue 3: 465-494.

Gordon, L.A., M.P. Loeb, W. Lucyshyn and R. Richardson. 2006. "2006 CSI/FBI Computer Crime and Security Survey". Computer Security Institute. Available online: http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf.

Grabosky, P.N. 2001. "Virtual Criminality: Old wine in new bottles?" *Social and Legal Studies*, Vol. 10, Issue 2: 243-249.

Hagan, F.E. 2006. Research Methods for Criminal Justice and Criminology (7th ed.). Boston, MA: Allyn and Bacon.

Hair Jr., J.F., R.E. Anderson, R.L. Tatham & W.C. Black. 1998. Multivariate Data Analysis. (5th ed.). Patparganj, Delhi, India: Pearson Education.

Heaphy, J.F. 1978. "The Future of Police Improvement." in Cohn, A. W. 1978. The Future of policing. *Criminal Justice System Annuals*, Vol. 9. Beverly Hills: Sage

Henderson, H. 2006. Internet predators. New York: Facts on File.

Hickman, M.J. and B.A. Reeves. 2006. "Local Police Departments 2003." Washington DC: Bureau of Justice Statistics. Available online: http://www.ojp.usdoj.gov/bjs/pub/pdf/lpd03.pdf.

Horrigan, J. and L. Rainie. 2006. "The Internet's Growing Role in Life's Major Moments." Pew Internet and American Life Project. Available online: http://www.pewinternet.org/PPF/r/181/report_display.asp

Internet Crime Complaint Center (2007). "2006 Internet Crime Report—Ohio." Internet Crime Complaint Center. Available online: http://www.http://www.ic3.gov/media/annualreport/2006/Ohio%202006%20Report.pdf.

Davies, P., Francis, P. and Jupp, V. 1999. "The Features of Invisible Crimes." in P. Davies, P. Francis and V. Jupp (eds.). Invisible Crimes: Their Victims and Their Regulation. London: Macmillan Press.

Kimberly, J.R. 1976. "Organizational Size and the Structuralist Perspective: A review, critique and proposal." Administrative Science Quarterly, Vol. 21, Issue 4: 571-597.

King, W.R. 1998. Innovativeness in American municipal police organizations. University of Cincinnati: Unpublished Doctoral Dissertation. Available online: http://www.uc.edu/criminaljustice/graduate/Dissertations/King.PDF.

King, W.R. 1999. "Time, Constancy, and Change in American Municipal Police Organizations." *Police Quarterly,* Vol. 2, Issue 3: 338-364.

King, W.R. 2009. "Organizational Failure and the Disbanding of Local Police Agencies." *Crime & Delinquency*, OnlineFirst: Available online at http://cad.sagepub.com/content/early/2009/09/08/0011128709344675.

Kovavich, G.L. and W. Boni. 2000. High-technology-crime investigator's handbook : working in the global information environment. Boston, MA: Butterfield-Heinemann.

Kowalski, M. 2002. "Cyber-crime: Issues, data sources, and feasibility of collecting police reported statistics." Canadian Center for Justice Statistics. Available online: http://www.statcan.ca/english/freepub/85-558-XIE/free.htm.

Langworthy, R.H. 1986. The Structure of Police Organizations. New York: Praeger.

Langworthy, R.H. 1989. "Do Stings Control Crime? An evaluation of a police fencing operation." *Justice Quarterly*, Vol. 6, Issue 1: 27-45.

Leiner, B.M., V.G. Cerf, D.D. Clark, R.E. Kahn, L. Kleinrock, D.C. Lynch, J. Postel, L.G. Roberts, and S. Wolff. 1997. "A Brief History of the Internet." Internet Society of America. Available online: http://www. isoc.org/internet/history/brief.shtml.

Lyman, M.D. 2002. The Police: An introduction. (2nd ed.). Upper Saddle River, NJ: Prentice Hall.

Madden, M. 2006. "Internet Penetration and Impact." Pew Internet and American Life Project. Available online: http://www.pewinternet.org/PPF/r/182/report_display.asp.

Maguire, E.R. 1997. "Structural Change in Large Municipal Police Organizations during the Community Policing Era." Justice Quarterly, Vol. 14, Issue 3: 701-730.

Maguire, E.R. 2003. Organizational Structure in American Police Agencies. Albany: State University of New York Press.

Massey, M. 1985. "Which 'New Technology'?" in M. Castells (ed.). High Technology, Space and Society, *Urban Affairs Annual Review*, Vol. 28. Beverly Hills, CA: Sage.

Mastrofski, S.D., R.R. Ritti, and D. Hoffmaster. 1987. "Organizational Determinants of Police Discretion: The case of drunk driving." *Journal of Criminal Justice,* Vol. 13, Issue 2: 387-402.

Maxfield, M.G. and E. Babbie. 1996. Research Methods for Criminal Justice and Criminology. Belmont, CA: Wadsworth.

McKenna, K.Y.A., A.S. Greene and M.E.J. Gleason. 2002. "Relationship Formation on the Internet: What's the big attraction." *Journal of Social Issues*, Vol. 58, Issue 1: 195-205.

McQuade III, S.M. 2006. Understanding and Managing Cybercrime. Boston: Pearson/Allyn and Bacon.

Mitchell, K.J., D. Finkelhor, and J. Wolak. 2001. "Risk factors and impact of online sexual solicitation of youth." *Journal of the American Medical Association*, Vol. 285, Issue 23: 1-4.

Molyneux, R. E. 2003. The Internet Under the Hood: An introduction to network technologies for information professionals. Westport, CT: Libraries Unlimited.

National Institute of Justice. 1999. "1999 Report on Cyberstalking: A new challenge for law enforcement and industry." Washington, DC: Department of Justice.

National Center for Missing and Exploited Children. 2007. "Cyber Tipline Fact Sheet." Available online: http://www.missingkids.com/en_US/documents/ CyberTiplineFactSheet.pdf.

Nye, N. and S. Hillygus. 2002. "Where Does Internet Time Come From? A reconnaissance." *IT & Society*, Vol. 1, Issue 2: 1-20.

Ohio Revised Code. (2006). Cincinnati, OH: Anderson. Available online: http://www.codes.ohio.gov.

Oliver, W.M. 2001. Community-Oriented Policing: A systematic approach to policing (2nd ed.). Upper Saddle River, NJ: Prentice Hall.

Ohio Peace Officers Training Commission. 2005. "A Statistical Profile of Ohio Peace Officers and Law Enforcement Agencies 2005." Available online: http://www.ag.state.oh.us/le/training/pubs/stat_profile_05.pdf.

Ostrom, E., R.B. Parks, and G.P. Whitaker. 1978. "Police Agency Size: Some evidence on its effects." *Police Studies,* Vol. 1, Issue 1: 34-46.

Pease, K. 2001. "Crime Futures: the challenge of crime in the information age" in D. S. Wall, ed. 2001. Crime and the Internet. London: Rutledge.

Pennings, J.M. 1998. "Structural Contingency Theory" in P.J.D. Drenth, H. Thierry and C.J. de Wolff, eds. 1996. Handbook of Work and Organizational Psychology: Volume 4, organizational psychology. East Sussex: Taylor and Francis Group.

Randala, R.R. 2004. "Cybercrime against Businesses: Pilot test results, 2001 Computer Security Survey" Washington, DC: U.S. Department of Justice Office of Justice Programs. Available online: http://www.ojp.usdoj.gov/bjs/pub/pdf/cb.pdf.

Rainie, L. 2001. "The commons of the tragedy: How the Internet was used by millions after the terrorattacks to grieve, console, share news, anddebate the country's response." Pew Internet and American Life Project. Available online: http://www.pewinternet.org/pdfs/PIP_Tragedy_Report.pdf.

Rainie, L., S. Fox, J. Horrigan, D. Fallows, A. Lenhart, M. Madden, M. Cornfield, C, Carter-Sykes. 2006. "The Mainstreaming of Online Life." in Trends 2005, Pew Research Center. Available online: http://pewresearch.org/pubs/206/trends-2005.

Rainie, L. and M. Madden. 2006. "Not looking for love: The state of romance in America." Pew Internet and American Life Project. Available online: http://www.pewinternet.org/pdfs/PIP_Romance_in_America_feb06.pdf.

Roberg, R. 1979. Police Management and Organizational Behavior: A Contingency Approach. New York: West.

Skinner, W.F. and A.M. Fream. 1997. "A Social Learning Analysis of Computer Crime among College Students." *Journal of Research in Crime and Delinquency*, Vol. 34, Issue 4: 495-518.

Slovak, J. 1986. Styles of Urban Policing: Organization, environment, and police styles in selected American cities. New York: New York University Press.

Swanson, C. 1978. "The Influence of Organization and Environment on Arrest Practices in Major U.S. Cities" *Policy Studies Journal*, Vol. 7: 390-398.

Stephenson, P. 2000. Investigating Computer Related Crime. Boca Raton, FL: CRC Press

Sykes, G.M. 1970. "The Future of Crime." Crime and Delinquency Issues: A Monograph Series. Rockville, MD: National Institute of Mental Health.

Tawil, D.D. 2000. "Ready? Induce. Sting!: Arguing for the government's burden of proving readiness in entrapment cases." *Michigan Law Review*, Vol. 98: 2371-2394.

Thompson, L. and J. Nadler. 2002. "Negotiation Via Information Technology: Theory and application." *Journal of Social Issues*, Vol. 58, Issue 1: 195-205.

Toffler, A., and H. Toffler. 1995. Creating a New Civilization: The Politics of the Third Wave. Nashville, TN: Turner.

Travis III, L.F. and Langworthy, R.H. 2008. Policing in America: A balance of forces. (4th ed.). Upper Saddle River, NJ: Pearson-Prentice Hall.

Tuchfarber, A.J. 1988. Ohio: Presidential Politics in "the Heart of it All." *Election Politics*. Vol. 5: 15-18. Cited in King, W.R. 2009. "Organizational Failure and the Disbanding of Local Police Agencies." *Crime & Delinquency*, OnlineFirst: Available online at http://cad.sagepub.com/content/ early/2009/09/08/0011128709344675.

Tyler, T.R. 2002. "Is the Internet Changing Social Life? It seems the more things change, the more they stay the same." *Journal of Social Issues*, Vol. 58, Issue 1: 195-205.

Vila, B. and C. Morris (eds.). 1999. The role of police in American society : a documentary history. Westport, CT: Greenwood.

Walker J. T. 1997. "Re-Blueing the Police: Technological Changes and Law Enforcement Practices" in M. L. Dantzker (ed.). Contemporary policing : personnel, issues, and trends

Wall, D.S. 2001. "Introduction: Crime and the Internet." In D. S. Wall (ed.). Crime and the Internet. London: Rutledge.

Walker, S. and Katz, C.M. 2011. The Police in America: An introduction. (7th ed.). New York: McGraw-Hill.

Warren, P. and M. Streeter. 2005. Cyber alert : How the world is under attack from a new form of crime. London: Vision.

Working to Halt Online Abuse (2007). "WHOA Comparison Statistics 2000-2006." Available online: http://www.haltabuse.org/resources/stats/Cumulative2000-2006.pdf

Wells, M., D. Finkelhor, J. Wolak and K. Mitchell. 2004. "Law Enforcement Challenges in Internet Child Pornography Crimes" *Sex Offender Law Report,* Vol. 5, Issue 4: 41-49.

Wells, L.E. and D.N. Falcone. 1992. "Organizational Variation in Vehicle Pursuits by Police: The impact of policy on practice." *CJ Policy Review*, Vol. 6, Issue 4: 311-333.

Wilson, J. Q. 1968. Varieties of Police Behavior: The management of law and order in eight communities. Cambridge, MA: Harvard University.

Wilson, J.Q. and G.L. Kelling. 1982. "Broken Windows: The police and neighborhood safety" The Atlantic Monthly, March: 29-38.

Wolak, J., D. Finkelhor, and K.J. Mitchell. 2004. "Internet-initiated sex crimes against minors: Implications for prevention based on findings from a national study." *Journal of Adolescent Health*, Volume 35, Issue 5: 424-433.

Wolak, J., K.J. Mitchell, and D. Finkelhor. 2006. "Online victimization of youth: Five years later." National Center for Missing & Exploited Children. Available Online: http://www.missingkids.com/en_US/publications/NC167.pdf

Ybarra, M. L., K. J. Mitchell, J. Wolak, and D. Finkelhor. 2006. "Examining characteristics and associated distress related to Internet harassment: Findings from the Second Youth Internet Safety Survey." *Pediatrics*, Vol. 118, Issue 4: 1169-1177.

Yamane, T. 1967. Statistics, An Introductory Analysis (2nd Ed). New York: Harper and Row.

Zhao, J., N.P. Lovrich; T.H. Robinson. 2003. "Community policing: is it changing the basic functions of policing? Findings from a longitudinal study of 200+ municipal police agencies." *Journal of Criminal Justice*, Vol. 29, Issue 5: 365-377.