Examining State and Local Law Enforcement Perceptions of Computer Crime

Thomas J. Holt, Adam M. Bossler, and Sarah Fitzgerald

The impact of computer-mediated communications and the Internet on all facets of human life has been well documented across the social sciences (Jewkes and Sharp 2003; Mann and Sutton 1998; Quinn and Forsyth 2005). Not only have these technologies changed the way that business and personal communications take place, but they have radically altered the capacity of offenders to engage in a variety of crimes (see Brenner 2008; McQuade 2006; Wall 2007). Electronic communications and the Internet have augmented or facilitated most forms of illegal behavior, including prostitution (Holt and Blevins 2007; Sharpe and Earle 2003; Soothhill and Sanders 2005), pedophilia (Durkin 1997; Durkin and Bryant 1999; Holt, Blevins, and Burkert 2010; Quayle and Taylor 2002), fraud (Burns, Whitworth, and Thompson 2004; Holt and Graves 2007; Holt and Lampke 2010; Newman and Clarke 2003) and piracy (see Higgins 2005; Higgins, Fell, and Wilson 2007; Hinduja 2001, 2003).

The economic impact of computer crimes is also substantial, affecting individuals and corporations alike. Businesses reported average losses of $500,000 in 2008 due to financial fraud incidents (Computer Security Institute 2008), while individual consumers lost an average of $575 to various types of fraud in 2009 (Internet Crime Complaint Center 2010). The music and movie industries also claim to have lost billions due to intellectual property theft and digital piracy (Higgins 2005; Higgins et al. 2007; Hinduja 2001, 2003; Motion Picture Association of America 2007). Furthermore, there are significant emotional and psychological consequences for victims of cyberstalking (Finn 2004; Holt and Bossler 2009) and children affected by pornography and pedophilia (see Berson 2003; Durkin and Bryant 1999).

In addition, computer-based terror attacks against all manner of targets have become an increasingly important issue for local law enforcement agencies across the nation (Aeilts 2005; Brenner 2008; Stambaugh et al. 2001). Many key resources in the public and private sector are linked to and depend on computer technology to function, including electrical grids, nuclear power plants, water infrastructure, and financial systems (Aeilts 2005; Denning 2001; Taylor, Fritsch, Liederbach, and Holt 2010). As a consequence, local law enforcement agencies must recognize and collaborate with private sector partners to protect and secure threats to critical infrastructure (see Brenner 2008; Taylor et al. 2010). Thus, law enforcement must be prepared to investigate a diverse range of offenses and offenders.

There is, however, a significant gap in our knowledge of law enforcement agencies' awareness, preparation, and attitudes toward computer crimes. Statistics on computer crimes are rarely collected by law enforcement agencies or reported in outlets such as the Uniform Crime Report or National Crime Victimization Survey. There are several reasons for this lack of data, including victim confusion over appropriate reporting agencies, concern that the incident is not important enough to report, and victims' inability to recognize when crimes have occurred (see Holt 2003; Speer 2000). This lack of statistical information makes it is difficult to estimate the true prevalence of computer crimes and how local law enforcement has or can respond to it. The lack of data at the local level is particularly significant, as these law enforcement agencies serve as primary first responders at all crime scenes, and their knowledge and ability to properly initiate an investigation has a significant impact on the way that cases are handled and investigated (see Burns et al. 2004; Goodman 1997; Hinduja 2004; McQuade 2006; Senjo 2004; Stambaugh et al. 2001). Thus, it is critical that researchers consider local agencies' attitudes toward the severity, frequency, and importance of computer crime offenses in order to assess training and resource needs, as well as their overall ability to properly investigate these offenses (see Burns et al. 2004; Hinduja 2004; McQuade 2006; Senjo 2004; Stambaugh et al. 2001).

This study seeks to fill this gap in our knowledge in two ways. First, we use data collected from a sample of state and local law enforcement officers and agents to understand their departments' and agencies' staffing and training for computer crime investigations and the handling of digital evidence. Second, we consider their perceptions of computer crime, their severity relative to street crimes, and knowledge of basic technology terms. The findings give insight into the preparedness of state and local police agencies to handle computer crime and the ways that their attitudes toward these offenses may affect investigations and officer behavior. The implications of this research for policy and future investigation are also considered.

Policing Computer Crime

There have been relatively few studies documenting the capacity for state and local law enforcement to properly investigate computer crime. One of the main studies considering police responses to computer crime is the Electronic Crime Needs Assessment for State and Local Law Enforcement report, published by the National Institute of Justice, which utilized data collected from a sample of 126 individuals from 114 agencies in 1998 (Stambaugh et al. 2001). Before conducting this study, the researchers recognized the complex issues surrounding the measurement of computer-based offenses and the lack of a universal definition for computer crime. Thus, they worked in collaboration with state and local agencies to develop a definition of "electronic crime" that refers to:

> fraud, theft, forgery, child pornography or exploitation, stalking, traditional white-collar crimes, privacy violations, illegal drug transactions, espionage, computer intrusions, or any other offenses that occur in an electronic environment for the purpose of economic gain or with the intent to destroy or otherwise inflict harm on another person or institution (Stambaugh et al. 2001, 2).

A similarly broad definition of cyberterrorism was developed, recognizing any "premeditated, politically motivated attack against information systems, computer programs and data … to disrupt the political, social, or physical infrastructure of the target" (Stambaugh et al. 2001, 2). The wide range of offenses included in these definitions was meant to provide a frame of reference for respondents and some standard to assess computer-based crime.

Using these definitions, Stambaugh et al. (2001) found a significant increase in computer crimes reported to law enforcement. At the same time, the respondents suggested that a substantial proportion of offenses were not being reported to law enforcement. Computer crime cases were given low priority across most agencies, unless they were child pornography or pedophile cases. This may have been a consequence of unsuccessful prosecutions, as many agencies felt that management, officers, and prosecutors appeared to have little knowledge and resources to adequately carry out computer crime investigations and prosecutions. Furthermore, respondents indicated the need for assistance with tools and training to better investigate these crimes. In fact, only half of all agencies had a formal electronic crime unit, and less than one third belonged to an interagency crime task force (Stambaugh et al. 2001).

Based on these findings, Stambaugh et al. (2001) identified ten critical needs to improve the capability of local and state law enforcement agencies to combat computer crimes. Specifically, these needs included (Stambaugh et al. 2001, 31–36).

1) **Public Awareness**: The public and private sectors needed to be better educated on the growing threat of computer crimes to decrease the likelihood of victimization.
2) **Data and Reporting**: Statistics and data collection on computer crime were needed to better understand computer crime prevalence and trends.
3) **Uniform training and certification courses**: Justice system actors, including prosecutors and judges, needed better training and certifications to effectively deal with computer crimes at all levels of the system.
4) **Onsite management assistance for electronic crime units and task forces**: State and local law enforcement agencies needed to develop computer crime units, as well as collaborative task forces, to better investigate computer crime cases.
5) **Updated laws**: Continuously updated legislation against computer crimes was needed to effectively prosecute cutting edge criminal acts and those crimes that cross jurisdictional boundaries.
6) **Cooperation with the high-tech industry**: The need for greater collaboration and communication with private industry was needed to increase reports of criminal incidents and improve high-tech crime training for law enforcement.
7) **Special research and publications**: A guidebook with information on training and investigative resources was needed to improve communications between investigators, forensic experts, management, and practitioners to deal with computer crime.
8) **Management awareness and support**: Law enforcement management and administrators needed to recognize the severity of computer crime and better support the investigation of these offenses.
9) **Investigative and forensic tools**: Better technological resources were needed to improve the investigation of computer crime cases, including budget conscious equipment to engender forensic examinations.
10) **Structuring a computer crime unit**: Research was needed to explore the needs and staffing issues present in the development of computer crime and forensic investigation units to create a best practices guide for law enforcement agencies.

Although a number of years have passed since the publication of the Electronic Crime Needs Assessment study (Stambaugh et al. 2001), there has been no systematic exploration of the impact of its policy recommendations or the general awareness of computer crime in local police agencies. A limited number of studies have examined the preparedness of law enforcement to examine specific forms of cybercrime, such as fraud (Burns et al. 2004), or cybercrime in specific areas (Hinduja 2004; Senjo 2004).

Burns et al. (2004) assessed the preparedness of law local enforcement to investigate Internet fraud. They found that most of the individuals responsible for filling out the survey believed online fraud was a serious problem (76.5 percent), but that law enforcement agencies in general did not consider Internet fraud to be a significant societal problem (41.0 percent). Most of them did not believe that they had sufficient funds to address Internet fraud (only 15.3 percent believed they had the necessary resources). Almost half of the agencies did not even have a computer crime division (46.7 percent). In fact, they would prefer Internet fraud laws to be enforced by federal (93.0 percent) or state law enforcement (69.7 percent) rather than local law enforcement (52.1 percent).

Hinduja (2004) considered the needs and preparedness of local law enforcement agencies in Michigan to deal with computer crimes. His study found that approximately twenty percent of the agencies (n=275) reported that they had one or more individuals trained to investigate these cases. Most agencies (66 percent), however, investigated less than ten computer crime cases in the year 2000. Of the computer crimes reported, harassment was the most common offense, followed by child pornography, solicitation of minors, identity theft, e-commerce fraud, and forgery. Thirty-six percent, however, reported that computer crimes detract attention from traditional crimes (Hinduja 2004).

The findings from Hinduja's (2004) research suggest that there is a need for greater preparation among law enforcement agencies to deal with computer crime, especially since some officers perceive computer crime cases to be insignificant. There has been little empirical research on police officer perspectives regarding the severity of computer crime: whether they think it is fundamentally different from "traditional" crime; the ways that law enforcement agencies have changed in response; and what they think should be done about these offenses. Senjo (2004) conducted one of the few studies examining line officers' perceptions of computer crime. In his sample of officers in a Western state, he found that officers, particularly younger officers with less experience, viewed pedophilia as the most serious computer crime that is occurring (Senjo 2004). Furthermore, officers believed computer criminals to be older males rather than young offenders. The reported officer perspectives were somewhat inconsistent with the larger empirical literature on computer crime, suggesting that there may be a gap in law enforcement knowledge of computer crime (Senjo 2004).

Taken as a whole, there is a critical need for greater research on local law enforcement awareness and training to deal with computer crimes. Few researchers have considered how the significant needs identified by the Electronic Crime Needs Assessment study (Stambaugh et al. 2001) have been met or improved on in local law enforcement agencies. Considering that the primary responsibility of investigating new types of crime falls on local law enforcement, it is critical that we understand how prepared first responders are to deal with computer crime and their attitudes toward the severity, frequency, and importance of these offenses. Such information can provide key policy recommendations to improve the training and resources available for local law enforcement agencies and increase the capability of first responders to appropriately handle computer crime cases.

Data

The data for this study were collected through an electronic survey solicitation administered by the Federal Law Enforcement Training Center (FLETC). This solicitation was delivered via email to approximately ten thousand individuals in state and local law enforcement agencies across the country who attended training classes related to computer crime and digital forensic examination. The solicitation provided a detailed introduction to the study, the relationship between the researchers and FLETC, and included a hyperlink to the online survey instrument. This process solicited 437 responses, less than five percent of the overall total of solicitations. Despite utilizing multiple measures to validate and encourage participation, the low response rate may have been a consequence of limited availability on the part of the responding officers. Alternatively, the respondents may have had some concerns over providing information on behalf of their agency on issues of training and caseloads. Although only 370 responses are needed to generalize to a solicitation of 10,000 (Krejcie and Morgan 1970), the volunteer bias precludes strong conclusions and does limit overall generalizability. Given the paucity of research in this area (see Hinduja 2004; Senjo 2004; Stambaugh et al. 2001), however, this sample provided a needed exploratory investigation into the capacity of state and local agencies to deal with computer crime.

Findings

Respondents were asked a battery of questions concerning their agency, computer crime investigations, and perceptions of computer crime offenders and activity. The survey instrument utilized measures adapted from multiple studies related to computer crime awareness in police agencies (see Goodman 1997; Hinduja 2004; Senjo 2004) and the general public (Furnell 2002). Each item will be explored and discussed in detail, starting with basic descriptive characteristics of the sample.

Demographic Composition

Basic descriptive information about the agency the respondent worked for was collected in lieu of demographic information from the respondent to maintain anonymity. In terms of agency size, 75.7 percent of the agencies had one hundred or less police officers serving in their agency (see Table 1). This is in fact under-representing smaller agencies as 93.9 percent of agencies have ninety-nine officers or fewer (BJS 2007). Thus, our sample consists of a higher percentage of larger agencies, which are more likely to have computer crime units and address computer crime, than is found in American policing. The geographic location of agencies was also collected using five bounded regions: the Midwest, South, Pacific, Northeast, and Mountain. Of the agencies surveyed, 28.5 percent indicated being in the Midwest, 33 percent in the South, 10.6 percent in the Pacific, 19.8 percent in the Northeast, and 8.1 percent in the Mountain region (see Table 1).

Table 1. Size and Geographic Location of Law Enforcement Agencies

Region	Less Than 20	20 to 100	101 to 200	201 to 500	501 to 1000	1001 to 5000	More Than 5000	Total
Midwest	48	39	6	4	1	4	0	102
South	36	51	11	12	2	6	0	118
Pacific	15	10	7	1	2	2	1	38
Northeast	27	20	7	9	1	4	3	71
Mountain	11	14	3	1	0	0	0	29
Total	137	134	34	27	6	16	4	358

Data on the number of individuals residing within the agency's geographic boundaries were also collected. Eleven percent of the agencies reported having one million or more individuals residing in their jurisdiction. Twenty-seven percent of the agencies had 5,001 to 20,000 citizens and twenty-two percent had five thousand or fewer individuals residing within their jurisdictional boundaries.

In order to understand the extent to which officers within departments handle computer-related crime issues, respondents were asked how many part-time officers or investigators they had within their agencies who were assigned to handle digital evidence. Results indicate that 76 percent of agencies had no part-time officers or investigators assigned to deal with digital evidence. Of those agencies with part-time personnel, the largest reported category (17.1 percent) was three to seven officers total. There were more agencies reporting full-time digital evidence handlers, as 44.7 percent had between one and four investigators. This is a significant improvement over previous research indicating that there have been some changes to increase law enforcement staffing for computer crime (see Goodman 1997; Hinduja 2004). It is important to note, however, that 23 percent of all agencies indicated that they had no part or full-time officers who could properly work with digital evidence. Thus, there are still some staffing issues concerning digital evidence at the state and local level.

Additionally, respondents were asked to assess the number of part-time and full-time officers assigned to the investigation of online crimes. This term was used in lieu of computer crime to assess any and all investigations that take place via the Internet. The overwhelming majority of departments (83.6%) had no part-time officers assigned to these investigations. This may be a function of the expense and manpower needed, making it more difficult to staff such roles with part-time investigators. Overall, 46 percent reported having between one to three full-time officers assigned to online crimes. At the same time, it is important to note that 38.7 percent of all responding agencies had no part or full-time officers trained to investigate online crime. This is a sizeable proportion, suggesting that there is still a need to increase the staff to support computer crime investigations in state and local agencies.

Respondents were also asked to estimate the percentage of officers within their agency that had received various training related to computer crime. Specifically, respondents were asked what percentage of their officers had been trained in handling digital evidence. Of those surveyed, 79.3 percent indicated that 20 percent or fewer of their officers had been trained in the handling of digital evidence (see Table 2). In terms of officers trained in investigating online crimes, the majority (88.1 percent) of agencies indicated that 20 percent or fewer of their officers had received such training. In terms of the percent of officers within each agency that had been trained in the handling of digital evidence, the Mid-

Table 2. The Percentage of Officers Trained for Digital Evidence and Computer Crime

Percentage of Officers	Digital Evidence (n-354)	Online Crime (n-345)
10	70.3	81.2
20	9.0	6.9
30–40	5.9	6.4
50–60	5.0	2.9
70–90	4.2	0.9
100	5.6	1.7

west had the greatest percentage, with nine agencies within this region indicating that 100 percent of their officers are trained in handling digital evidence. This finding is in keeping with previous research (e.g., Hinduja 2004) and suggests that there are slight improvements taking place to change the investigative power of state and local agencies to deal with computer crime.

Investigations

Respondents were asked to indicate whether or not their agency actively investigated various forms of economic, sexual, and hacking-related computer crimes (see Table 3 for detail). The most common type of investigation conducted involved identity theft (79.2 percent), followed by fraud (71.9 percent) and online harassment (71.8 percent) (see Hinduja 2004 for similar finding on harassment). This is a distinct shift from previously identified investigative priorities, as sex offenses appeared to be the dominant crime reported to state and local agencies (Stambaugh et al. 2001). Such a change may be a reflection of the increasing use of the Internet for financial transactions and information, as well as improved awareness of this type of crime in the general population (see Burns et al. 2004; Holt and Lampke 2010). Child pornography and the solicitation of minors were also somewhat common as more than half of the responding agencies conduct such investigations. The least examined form of computer crime were hacking and computer intrusion cases. This results from both the difficulty in investigating these crimes as well as the cross-state and international dynamics of computer hacking, as offenders can reside anywhere in the country or world and victimize multiple machines in any location (see Brenner 2008; McQuade 2006; Taylor et al. 2010; Wall 2007). The

Table 3. Types of Computer Crimes Investigated by State and Local Agencies

	Yes	No
Identity theft (n=355)	79.2	20.8
Fraud (n=356)	71.9	28.1
Harassment (n=358)	71.8	28.2
Child porn (n=358)	61.7	38.3
Solicitation of children (n=358)	51.7	48.3
Sex crimes (n=357)	42.0	58.0
Hacking/intrusion (n=353)	32.0	68.0

jurisdictional issues that can arise make hacking investigations more likely to fall under federal law enforcement agency purview.

Respondents were also asked to identify how many cases their agency had dealt with in the last twelve months involving online crime and digital evidence, to give some insight into the prevalence of these issues in state and local agencies (see Table 4). With regard to digital evidence, 70 percent of the agencies had nineteen or fewer cases involving digital evidence within the last twelve months. 18.7 percent had no cases within the prior year that had digital evidence. Thus, there are relatively few cases being investigated with digital evidence by these agencies among first responders, in keeping with previous research. Respondents were also asked how many digital evidence cases were cleared by arrest in the past twelve months (results not shown). Of the agencies involved, 33.5 percent indicated zero arrests, while 25.9 percent said that there were one or two cases that resulted in an arrest. Only 5 percent of agencies indicated that they had made one hundred or more arrests from cases involving the handling of digital evidence. Thus, despite the use of digital forensic techniques, there appears to be a relatively small number of cases cleared by arrest at the local level.

Similar patterns were identified concerning cases involving some form of computer crime, such as computer hacking or sex offenses (see Table 9.4). Specifically, 75.2 percent reported they had nineteen or fewer online crime cases within the previous year, more than half of the agencies (57.2 percent) had five or fewer cases, and 27.9 percent stated they had zero. The number of computer crime cases cleared by arrest was much smaller than in the digital evidence category. Most agencies (65 percent) had less than two cases cleared by

Table 4. Number of Active Cases Involving Digital Evidence or Computer Crime

	Digital Evidence		Online Crime	
Number of Cases	N	Percentage	N	Percentage
0 cases	67	18.7	96	27.9
1–2 cases	54	15.0	53	15.4
3–5 cases	67	18.7	48	13.9
6–19 cases	63	17.6	62	18.0
20–99 cases	49	13.7	58	16.9
100–800 cases	40	11.2	23	6.7
1000 or more cases	18	5.0	4	1.2
Total	358	100	344	100

arrest, which is sensible given the relative anonymity the Internet provides for offenders (see McQuade 2006; Wall 2007).

Attitudes toward Computer Crime

Respondents were also asked to indicate their level of agreement with various statements related to computer crime, including offender behaviors, victim impacts, and citizen awareness of this problem (see Table 5). One of the most significant points of agreement (98.1 percent) was in support of the statement, “Computer crime is a serious problem in American society.” This suggests that officers recognize the seriousness of computer crime. Clearly, a part of this is due to the fact that most of them (92.8 percent) agreed with the following statement, “Computers allow individuals to feel less responsible for their actions, increasing the likelihood of crime.” In addition, 82.1 percent believed that attacks on computer systems pose a threat equal to or greater than physical attacks. This indicates that law enforcement agencies are aware of the danger posed by acts of cyberterror, particularly in the post 9/11 world.

Most respondents, however, felt that individuals in their community did not recognize the risk that they face from these offenses. Only 15.1 percent agreed that, “Citizens in our community understand the risk of computer crime.” This is surprising in light of the significant recognition of cybercrime as a problem among law enforcement agencies. Thus, there may be a discon-

Table 5. Officers' Reported Attitudes Toward Computer Crimes

Statement	Agree	Disagree
Computer crime is a serious problem in American society.	98.1	1.9
Computers allow individuals to feel less responsible for their actions increasing the likelihood of crime.	92.8	7.2
Budget constraints limit our ability to investigate computer crimes.	89.4	10.6
Attacks on computer systems pose a threat equal to or greater than physical attacks.	82.1	17.9
Computer crimes have a greater impact in corporate settings rather than in home settings.	69.9	30.1
The majority of computer crimes are perpetrated by individuals in their teens and twenties.	48.5	51.5
Computer crimes detract officers' attention from street crimes.	47.9	52.1
Computer criminals often reside in foreign countries rather than the US.	45.9	54.1
Computer crime occurs more frequently in businesses rather than among home users.	41.5	58.5
Convicted hackers should be allowed to work in computing jobs.	18.1	81.9
Citizens in our community understand the risk of computer crime.	15.1	84.9
Convicted hackers should be allowed to have a computer at home.	13.2	86.8

nect between law enforcement and citizens' perceptions of the severity of computer crime.

A majority of the respondents (89.4 percent) also believed that budget constraints limited their ability to investigate computer crimes (see Hinduja 2004; Stambaugh et al. 2001). Coupled with their beliefs that computer crime is a serious problem, this implied that these officers believed that more funding would lead to better investigations of computer crime. Almost half of the respondents (47.9 percent), however, responded that computer crimes detract officers' attention from street crimes, possibly implying that this issue has not improved since earlier studies and commentaries (Goodman 1997; Hinduja 2004; Stambaugh et al. 2001). Thus, budget constraints might be a strong factor in why local law enforcement does not focus more on computer crimes. Also, state and local law enforcement agencies' interest in investigating these crimes may not be as strong as their belief that it is a serious problem.

There were, however, some disagreements among the respondents as to the types of offenders who engage in computer crimes and who is more likely to be victimized. A little less than half of the respondents (45.9 percent) agreed that computer criminals often reside in foreign countries, indicating that half of the respondents believed that most of our computer crime problem is homegrown. Half of the respondents (48.5 percent) agreed that most computer criminals are in their teens and twenties. This is a shift from previous studies, which found greater support for the contention that computer criminals are older individuals (Furnell 2002; Senjo 2004). The research literature is mixed concerning these issues, as computer hackers are largely younger males (Brenner 2008; Jordan and Taylor 1998; Holt 2007), while there are few metrics on the demographic composition of pedophiles and online sex offenders (see Quayle and Taylor 2002). The relative split noted in this data may be a reflection of increasing awareness of the variation in offender characteristics. In addition, only 41.5 percent believed that businesses were more likely to be the victims of computer crime relative to home users. At the same time, almost 70 percent agreed that computer crime had a greater impact in corporate settings. Thus, the respondents believed that individuals were more likely to be victimized, but the consequences were greater for corporations (see also Furnell 2002).

Furthermore, the majority of the sample did not support the notion that convicted computer hackers should be allowed to work in computing jobs (81.9 percent) or have a computer in their homes (86.8 percent). This finding is similar to research on the general population's attitudes toward computer crime offending (see Furnell 2002). It is important to note, however, that reformed hackers play important roles in the computer security community, and can assist in the investigation of computer crimes (see Furnell 2002; Holt 2007; Taylor et al. 2010). These individuals could also facilitate training and assist state and local law enforcement in light of the dearth of officers and resources to investigate these crimes. Thus, local law enforcement agencies desire to restrict hackers' access to technology may actually be problematic given their capacity to assist policing agencies.

Perceptions of Computer Crime Offending

In order to assess how law enforcement agencies perceive computer crimes relative to terrestrial crimes, respondents were asked to rank the severity of a variety of offenses on a five-point scale from least serious (1) to most serious (5). The mean scores for each form of crime are presented in Table 6 and provide an interesting perspective on the perceived impact of both computer and real world crimes and the relationships between these offenses (see also Senjo 2004).

Table 6. Perceived Severity of Computer Crimes

Offense Type	Mean Severity	N
Stealing something worth less than $5 dollars	2.09	357
Using someone else's wireless connection	2.92	355
Unauthorized copying of media	2.97	358
Stealing something worth more than $50	3.19	357
Unauthorized copying of software	3.26	358
Purposely damaging or destroying property	3.50	358
Harassment over the Internet	3.68	358
Breaking into a vehicle or building to steal something	3.82	357
Viewing someone else's electronic data without permission	3.85	358
Hitting someone without any reason	3.88	358
Viruses and malicious software infection	4.20	358
Electronic theft of money from accounts	4.46	357
Selling hard drugs such as heroin, cocaine, or meth	4.49	358
Terrorist attacks against electronic targets (cyberterror)	4.59	359
Terrorist attacks against physical targets	4.84	356
Child pornography and sexual solicitation	4.86	358

The respondents considered stealing something worth less than five dollars to be the least serious crime of the crimes examined. In fact, they considered five different types of theft—stealing something worth less than five dollars; using someone else's Internet connection; media and software piracy; and stealing something more than fifty dollars—to be the least serious crimes overall. Thus, less serious forms of crime and relatively equal, regardless of whether they based in the physical or virtual world. Purposely damaging property was considered slightly more severe than the minor forms of theft, with harassment via the Internet considered the next severe. The respondents indicated that threats, although virtual with possibly no physical contact ever between victim and offender, are still considered more serious than real world property damage.

A similar clustering of severity was noted for breaking into a vehicle or building to steal something, viewing electronic data without permission, and hitting someone without any reason. The relationship between burglary and hacking has been proposed by a variety of scholars, and the appearance of this relationship suggests law enforcement agencies may share this point of view (see Wall 2001). In addition, it appears that the respondents equated serious forms of privacy violation (e.g., having electronic data viewed and having something stolen from a vehicle or building) to be equivalent of minor forms of violence. Malicious software infections, such as the spread of viruses, however, were ranked higher than these offenses. This is sensible given that malware can be used as an attack platform for various types of hacking and theft (Bossler and Holt 2009; Brenner 2008; Taylor et al. 2010), as well as damage computer systems and networks. This finding suggests state and local law enforcement agencies recognize the severity of more significant hacker-related computer crimes.

The mean scores for electronic theft of money and the sale of hard drugs were also relatively similar. Both offenses have a significant impact, though for very different reasons. The financial impact of electronic theft for victims can be quite substantial, and are complex offenses for law enforcement agencies to investigate and clear by arrest (see Internet Crime Complaint Center 2010; Newman and Clarke 2003). Drug sales, however, have significant negative consequences for drug abusers and the larger community, including increased rates of disorder, theft, prostitution, and lethal violence (see Harocopos and Hough 2005). These issues may drive the similar perceived impact of these offenses.

Finally, officers reported the following crime types as the most severe: child pornography and sexual solicitation and physical and cyber terrorist attacks. Though there are clear and significant threats posed by virtual and real world acts of terror, it is surprising that child offenses are perceived as having greater severity than terror attacks. The significant social stigma associated with child sex offenses (see Durkin 1997; Durkin and Bryant 1999; Holt et al. 2010) may, however, account of this ranking. Specifically, child victims can be easily taken advantage of, and coerced into acts due to their innocence and naïveté (Durkin 1997; Durkin and Bryant 1999). Regardless, these findings suggest that local law enforcement agencies perceive there to be significant overlap between virtual and terrestrial crimes.

In addition, the respondents were asked to indicate the frequency with which certain computer crimes take place, ranging from never (1) to very frequently

(6). The mean scores for the frequency of each offense are presented in Table 7. The high mean scores suggest that local agencies feel computer crimes occur with some regularity, with acts of cyber-terror performed least often (4.58). Electronic theft and viewing data without permission are also perceived to occur with some frequency, which may be a reflection of the increasing investigation of these offenses at the state and local level (see Burns et al. 2004). The perceived prevalence of harassment and malware infections may be a consequence of increasing media and research coverage which suggest these offenses are increasing yearly (see Bossler and Holt 2010; Finn 2004; Holt and Bossler 2009; Taylor et al. 2010).

Table 7. Perceived Frequency of Computer Crimes

Offense Type	Mean Frequency	N
Terrorist attacks against electronic targets (cyber-terror)	4.58	359
Viewing someone else's electronic data without permission	4.83	359
Electronic theft of money from accounts	4.96	358
Harassment over the Internet	5.10	358
Viruses and malicious software infection	5.11	359
Child pornography and sexual solicitation	5.35	359
Unauthorized copying of software	5.38	359
Unauthorized copying of media	5.54	359

Respondents ranked the most common forms of computer crime to be software and media piracy. Empirical research on digital piracy suggests this is a prevalent offense that cuts across race, age, and economic conditions (see Higgins 2005; Higgins, Fell, and Wilson 2007; Hinduja 2001, 2003; McQuade 2006; Wall 2007). Thus, state and local agencies appear to have a perspective on computer crime that conforms to the broader research literature on computer offending generally.

Respondents were also asked to assess the threat of cyberterror attacks posed by various countries on a scale from least serious (1) to most serious (5) (see Table 8). The countries selected for this inventory were based in part on reports from various media and research on national participation in computer crime and attacks against military and private targets (see Brenner 2008; Holt,

Table 8. Perceived Threat of Cyberterror Attacks from Multiple Nations

Country	Mean Frequency	N
Brazil	2.91	357
Egypt	3.22	353
Afghanistan	3.33	355
Romania	3.33	357
Japan	3.36	356
Iraq	3.45	356
Russia	3.74	356
Iran	3.92	356
China	4.32	359

Soles, and Leslie 2008; Taylor et al. 2010). Additionally, a number of Middle Eastern nations were included as controls since they have limited participation in actual cyber-attacks, but heavy participation in e-jihad as a means of recruitment and information sharing for terror groups (see Brenner 2008; Taylor et al. 2010).

Brazil was ranked the least threatening nation overall by respondents. This could be a reflection of a lack of knowledge about the hacking landscape in Brazil, or a more general consequence of the fact that Brazilian hackers regularly target South American financial institutions and customers rather than those in other nations (Taylor et al. 2010). Egypt, Afghanistan, Romania, Japan, and Iraq were all considered moderate threats. It appears that some of the countries in this group might be viewed as threats more because of the war on terrorism and law enforcement perceptions that these countries desire to attack the United States rather than their actual ability to strike critical infrastructure.

Russia was ranked as a high threat, but placed below Iran. Russian hackers have engaged in a variety of attacks against US financial institutions and critical infrastructure (see Holt et al. 2008; Honeynet Research Alliance 2003) as well as cyber-attacks against neighboring nations, such as Estonia and Georgia (Brenner 2008; Jaffe 2006; Landler and Markoff 2008). Few, if any, attacks have been attributed to Iran. Thus, this threat ranking appears to stem from regular reports about the nuclear threat posed by Iran and its posturing toward other nations around the world. Finally, China was ranked as the highest overall threat in keeping with multiple media reports of high level intrusions by Chinese hackers into sensitive networks in governments around the world (Holt et al. 2008; Taylor et al. 2010). Thus, local and state law enforcement agencies appear to share some perspectives on the broader landscape of cyberthreats, but also appear to assign too high of threats to countries based more on the desire to attack the United States than their ability to complete such an intrusion.

Awareness of Technology

To gain some perspective on state and local officers' knowledge of computer technology and offending, respondents were presented with various technology-specific terms and asked to identify whether they were familiar with the term, unsure of its meaning, or had never heard it before (see Table 9). The findings indicate that most respondents felt that they knew the meanings of many essential terms needed to understand both basic computing software and computer crimes. A majority of the officers reported knowledge of the terms spam,

Table 9. Knowledge of Terms Related to Computer Technology and Computer Crime

Term	I have a good idea what this term means	Not really sure what this term means	I have never heard this term
Identity theft	98.6	1.1	0.3
Viruses	97.7	2.3	0.0
Spam	96.6	3.4	0.0
Firewall	95.5	4.5	0.0
Spyware	93.8	5.9	0.3
Cookies	89.8	8.8	1.4
Cyberstalking	85.2	13.7	1.1
Phishing	79.3	13.1	7.7
Adware	78.3	17.7	3.9
Podcasts	65.4	28.6	5.9
Carding	18.9	44.5	36.6

firewall, spyware, and cookies. This is sensible given that these terms are commonly used with regard to the Internet and computer security as a whole (Taylor et al. 2010; Wall 2007). There was, however, less recognition for the terms Adware and podcast. Thus, state and local agencies have a grasp of the basic terms that support web browsers and Internet use.

Respondents also appeared to be familiar with most terms related to either a type of computer crime or an attack tool. For example, identity theft, virus, and cyberstalking were identified by most respondents. The reported knowledge of identity theft and cyberstalking may be related to the prevalence of investigations at the local level and in media accounts. Phishing, where criminals attempt to obtain financial information from unwitting victims via email (James 2005), was identified by fewer officers (79 percent). The one item most respondents did not know was "carding," where individuals buy and sell stolen personal information for the purposes of fraud and theft (Holt and Lampke 2010; Honeynet Research Alliance 2003). This may be a consequence of the relatively recent emergence of this crime and that it is mostly investigated by federal agencies due to the international scope of these offenses. Regardless, these findings suggest that local policing officers have a strong awareness of computer crime terms and that their knowledge has increased over the last decade (Goodman 1997).

In addition, respondents appeared to have some recognition of terms related to cyber-terrorism (see Table 10). Many of the respondents knew the term "critical infrastructure," which is a positive finding given the prominence

Table 10. Knowledge of Terms Related to Computer Technology and Computer Crime

Term	I have a good idea what this term means	Not really sure what this term means	I have never heard this term
People's Liberation Army	78.5	17.8	3.7
Critical Infrastructure	77.3	15.3	7.4
E-jihad	70.5	20.2	9.4
Information Warfare	47.6	40.8	11.5
Firesale	34.7	43.8	21.5

of this phrase in recent years related to physical terror attacks (see Taylor et al. 2010). Most respondents had also heard of the People's Liberation Army and the term "e-jihad." This is encouraging since these phrases are related to two distinct groups involvement in cyberterror. The People's Liberation Army, the name of the Chinese military, is responsible for several serious computer intrusions against Department of Defense computer networks, power grids, and other systems (Brenner 2008). E-jihad is a phrase related to the development of terror groups' usage of the internet for various activities, from recruitment to misinformation to attacks against different targets (see Brenner 2008; Taylor et al. 2010).

Knowledge of the term "information warfare" was much lower, with less than half of all respondents recognizing this word. The phrase "information warfare" is primarily used in the military community to represent any behavior involving the use of or gathering of information to gain advantage over another party (see Taylor et al. 2010). This can include acts of cyberterrorism or data theft, and comprises a significant potential overlap between law enforcement practices and military activity. The relative concentration of this term among military actors may, however, account for the lack of awareness in state and local law enforcement agencies. Finally, the term "firesale" was included as a control because it is not a phrase used in the academic or policing communities. Instead, this term is used in popular media to describe a cataclysmic series of cyberattacks. Since only 34.7 percent of respondents knew this term, it appears that the respondents have not been significantly swayed by media accounts of cyberterror attacks. Taken as a whole, the respondents appear to have some sound understanding of key phrases related to cyberterror as well as computer crime generally.

Discussion and Conclusions

Despite the increasing body of research on computer crime offending and victimization, few studies have considered the capacity of local law enforcement agencies to investigate and combat these crimes (see Burns et al. 2004; Hinduja 2004; McQuade 2006; Senjo 2004; Stambaugh et al. 2001; Taylor et al. 2010). This study attempted to address this issue through an examination of 437 state and local law enforcement agents and officers to understand their investigative capabilities and perspectives on computer crime. As a whole, the findings suggest that law enforcement agencies have shifted their investigative resources to become more actively involved in financial offenses than in the past (see Burns et al. 2004; Hinduja 2004; Senjo 2004; Stambaugh et al. 2001). While local agencies are still investigating sex offenses, there were more agencies suggesting they investigate economic-driven computer crimes. Such a finding is a positive indicator, given the tremendous economic impact of computer-based fraud for businesses and individuals alike (Internet Crime Complaint Center 2010; Newman and Clarke 2003; Wall 2007).

At the same time, the lack of agencies investigating computer hacking and intrusions is in keeping with previous research on policing (see Hinduja 2004; Stambaugh et al. 2001). This may, however, be a function of limited resources and jurisdictional issues that complicate reporting and proper exploration (Brenner 2008; Taylor et al. 2010; Wall 2007). Additionally, the relative paucity of cleared and active cases involving both computer crimes and digital evidence indicate that these offenses are relatively underexamined at the local level (see Hinduja 2004). This exploratory finding, however, demands greater research, and emphasizes the need for improved statistical reporting to better comprehend the problem of computer crime (Brenner 2008; Hinduja 2004; Holt 2003; Wall 2007).

The attitudinal results suggest that state and local law enforcement may have improved their situational awareness and preparation to deal with computer crime cases. Specifically, local agencies have an increased overall recognition of the serious threat computer crimes pose. Additionally, the mixed agreement surrounding victim impact indicates that police officers may understand that certain offenses, such as hacking or fraud, may have a greater impact for businesses, while stalking could impact individuals more heavily. Finally, the respondents' significant agreement with the need for increased funding to support the investigation suggests that there is a need for greater resource allocation to improve the local response to computer crimes (Hinduja 2004; Stambaugh et al. 2001).

The perceived severity of computer offending relative to street crimes also gives some valuable insights into the nature of computer crime investigation. The relatively low significance of minor theft and piracy suggests that these offenses may have minimal priority among law enforcement agencies. This could be a function of the lack of victims or the underreporting of these offenses, particularly piracy where there is no distinct or immediate individual affected (see Hinduja 2001). The relatively high severity of malware is also a positive finding, as malware can be used in a variety of ways by computer hackers and attackers to engage in different forms of crime (see Bossler and Holt 2009; Brenner 2008; Taylor et al. 2010). Additionally, the noted severity of both physical and computer-based terror attacks suggests that state and local agencies understand the need to reorient some of their priorities in order to act as first responders to serious incidents, particularly in the wake of the 9/11 attacks (see Brenner 2008). Finally, the extremely high placement of child pornography is in keeping with previous research (see Senjo 2004) and reflects the social concerns surrounding this type of offense (see Holt et al. 2010).

Additionally, the noted variation in knowledge of various computer technology and crime terms indicates that law enforcement officers have some awareness of the resources that undergird the Internet and web browsers. In addition, the recognition of the more prominent forms of computer crime, including spam, phishing, and cyberstalking, provides some support for an improved response to computer crime at the local level. The fact that most officers ranked Russia and China as the greatest threats toward US critical infrastructure is also instructive, as this idea has been promulgated in both research and popular media (see Brenner 2008; Denning 2001; Holt et al. 2008; McQuade 2006; Taylor et al. 2010; Wall 2007). Thus, local agencies appear to have some grounding in the threats and problems operating in virtual environments today.

Taken as a whole, this study indicates an improvement in state and local law enforcement responses and training to deal with various computer crimes. In the years following the recommendations made by the National Institute of Justice report (Stambaugh et al. 2001), it appears that there is greater recognition of the problem of computer crime among first responders. The preliminary and exploratory nature of these findings, due to the response rate, however, clearly requires replication to be verified and validated. We caution others not to make strong conclusions from our findings, but rather examine the trends found. In addition to increasing the size and representativeness of the sample, future researchers will want to compare and contrast line officers with little to no training in digital forensics and computer crime investigation with officers who have more extensive training. Finally, sampling managers within law enforcement agencies is needed to consider the acceptance and knowledge of individuals who control the economic and procedural dynamics within state and local agencies. Such research can provide critical information on the greater landscape of law enforcement and their ability to adapt and respond to the growing problem of computer crime in modern society.

References

Aeilts, Tony. “Defending against cybercrime and terrorism,” *FBI Law Enforcement Bulletin* 74 (2005): 14–20.

Berson, Ilene R. “Grooming cybervictims: The psychosocial effects of online exploitation of youth,” *Journal of School Violence* 2 (2003): 5–18.

Bossler, Adam M., and Thomas J. Holt. “On-line activities, guardianship, and malware infection: An examination of routine activities theory,” *International Journal of Cyber Criminology* 3 (2009): 400–420.

Brenner, Susan W. *Cyberthreats: The Emerging Fault Lines of the Nation State.* New York: Oxford University Press, 2008.

Bureau of Justice Statistics. *Census of State and Local Law Enforcement Agencies, 2004.* Washington, DC: Government Printing Office, 2007.

Burns, Ronald G., Keith H. Whitworth, and Carol Y. Thompson. "Accessing law enforcement preparedness to address Internet fraud," *Journal of Criminal Justice* 32 (2004): 477–493.

Computer Security Institute. *Computer Crime and Security Survey, 200*8.Accessed June 3, 2009. http://www.cybercrime.gov/FBI2008.pdf.

Denning, Dorothy E. "Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy." In *Networks and Netwars: The Future of Terror, Crime, and Militancy*, eds. John Arquilla and David F. Ronfeldt, 239–288. Santa Monica, CA: Rand 2001.

Durkin, Keith F. "Misuse of the Internet by pedophiles: Implications for law enforcement and probation practice," *Federal Probation* 61 (1997): 14–18.

Durkin, Keith F., and Clifton D. Bryant. "Propagandizing pederasty: A thematic analysis of the on-line exculpatory accounts of unrepentant pedophiles," *Deviant Behavior* 20 (1999): 103–127.

Finn, Jerry. "A survey of online harassment at a university campus," *Journal of Interpersonal Violence* 19 (2004): 468–483.

Furnell, Steven. *Cybercrime: Vandalizing the Information Society*. Boston: Addison-Wesley, 2002.

Goodman, Marc D. "Why the police don't care about computer crime," *Harvard Journal of Law and Technology* 10 (1997): 465–494.

Harocopos, Alex, and Mike Hough. "Drug dealing in open-air markets," *Problem-Oriented Guides for Police* No. 31. Washington D.C.: U.S. Department of Justice Office of Community Oriented Policing Services, 2005.

Higgins, George E. "Can low self-control help with the understanding of the software piracy problem?" *Deviant Behavior* 26 (2005): 1–24.

Higgins, George E., Brian D. Fell, and Abby L. Wilson. "Low self-control and social learning in understanding students' intentions to pirate movies in the United States," *Social Science Computer Review* 25 (2007): 339–357.

Hinduja, Sameer. "Correlates of Internet software piracy," *Journal of Contemporary Criminal Justice* 17 (2001): 369–382.

Hinduja, Sameer. "Trends and patterns among software pirates," *Ethics and Information Technology* 5 (2003): 49–61.

Hinduja, Sameer "Perceptions of local and state law enforcement concerning the role of computer crime investigative teams," *Policing: An International Journal of Police Strategies & Management* 27 (2004): 341–357.

Holt, Thomas J. "Examining a transnational problem: An analysis of computer crime victimization in eight countries from 1999 to 2001," *International Journal of Comparative and Applied Criminal Justice* 27 (2003): 199–220.

Holt, Thomas J. "Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures," *Deviant Behavior* 28 (2007): 171–198.

Holt, Thomas J., and Kristie R. Blevins. "Examining sex work from the client's perspective: Assessing johns using online data," *Deviant Behavior* 28 (2007): 333–354.

Holt, Thomas J., Kristie R. Blevins, and Natasha Burkert. "Considering the pedophile subculture on-line," *Sexual Abuse: Journal of Research and Treatment* 22 (2010): 3–24.

Holt, Thomas J., and Adam M. Bossler. "Examining the applicability of lifestyle-routine activities theory for cybercrime victimization," *Deviant Behavior* 30 (2009): 1–25.

Holt, Thomas J. and Danielle C. Graves. "A qualitative analysis of advanced fee fraud schemes," *The International Journal of Cyber-Criminology* 1 (2007): 137–154.

Holt, Thomas J. and Eric Lampke. "Exploring stolen data markets on-line: Products and market forces," *Criminal Justice Studies* 23 (2010): 33–50.

Holt, Thomas J., Joshua B. Soles, and Lyudmila Leslie. "Characterizing malware writers and computer attackers in their own words," Proceedings of the 2008 International Conference on Information Warfare and Security, Peter Kiewit Institute, University of Nebraska Omaha.

Honeynet Research Alliance. "Profile: Automated Credit Card Fraud," *Know Your Enemy Paper* series, 2003. Accessed July 20, 2008. http://www.honeynet.org/ papers/profiles/cc-fraud.pdf.

Internet Crime Complaint Center. *IC3 2009 Internet Crime Report.* Accessed March 24, 2010. http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf.

Jaffe, Greg. "Gates Urges NATO Ministers To Defend Against Cyber Attacks," *The Wall Street Journal On-line.* June 15, 2006. Accessed July 19, 2007. http://online.wsj. com/article/SB118190166163536578.html?mod=googlenews_wsj.

James, Lance. *Phishing Exposed.* Rockland: Syngress, 2005.

Jewkes, Yvonne, and Keith Sharp. "Crime, deviance and the disembodied self: transcending the dangers of corporeality," In *Dot.cons: Crime, deviance and identity on the* Internet, ed. Yvonne Jewkes, 1–14. Portland, OR: Willan Publishing, 2003.

Jordan, Tim, and Paul Taylor. "A Sociology of Hackers," *The Sociological Review* 46 (1998): 757–80.

Krejcie, Robert V. and Daryle W. Morgan. "Determining sample size for research activities," *Educational and Psychological Measurement*, 30 (1970): 607–610.

Landler, Mark and John Markoff. "Digital Fears Emerge After Data Siege in Estonia," *The New York Times*, May 24, 2007. Accessed July 17, 2009. www.nytimes.com/2007/ 05/29/technology/29estonia.html.

Mann, David, and Mike Sutton. "Netcrime: More change in the organization of thieving," *British Journal of Criminology* 38 (1998): 201–229.

McQuade, Sam. "Technology-enabled crime, policing and security," *Journal of Technology Studies* 32 (2006): 32–42.

Motion Picture Association of America. *2005 Piracy fact sheet.* Accessed December 12, 2007. http://www.mpaa.org/researchStatistics.asp.

Newman, Grame, and Ronald Clarke. *Superhighway robbery: Preventing e-commerce crime.* Cullompton: Willan Press, 2003.

Quayle, Ethel, and Max Taylor. "Child pornography and the Internet: Perpetuating a cycle of abuse," *Deviant Behavior* 23 (2002): 331–361.

Quinn, James F., and Craig J. Forsyth. "Describing sexual behavior in the era of the internet: A typology for empirical research," *Deviant Behavior* 26 (2005): 191–207.

Senjo, Scott R. "An analysis of computer-related crime: Comparing police officer perceptions with empirical data," *Security Journal* 17 (2004): 55–71.

Sharp, Keith, and Sarah Earle. "Cyberpunters and cyberwhores: prostitution on the Internet." In *Dot Cons. Crime, Deviance and Identity on the Internet*, ed. Yvonne Jewkes, 36–52. Portland, OR: Willan Publishing, 2003.

Soothhill, Keith, and Teela Sanders. "The geographical mobility, preferences and pleasures of prolific punters: A demonstration study of the activities of prostitutes' clients," *Sociological Research On-Line* 10 (2005). Accessed October 10, 2005. http://www.socresonline.org.uk/10/1/soothill.html.

Speer, David L. "Redefining borders: The challenges of cybercrime," *Crime, Law, and Social Change* 34 (2000): 259–273.

Stambaugh, Hollis, David S. Beaupre, David J. Icove, Richard Baker, Wayne Cassady, and Wayne P. Williams. *Electronic crime needs assessment for state and local law enforcement.* Washington, DC: National Institute of Justice, 2001. NCJ 186276.

Taylor, Robert W., Eric J. Fritsch, John Liederbach, and Thomas J. Holt. *Digital Crime and Digital Terrorism, 2nd edition.* Upper Saddle River, NJ: Pearson Prentice Hall, 2010.

Wall, D. S. "Cybercrimes and the Internet," pp. 1–17 in *Crime and the Internet*, edited by D. S. Wall. New York: Routledge, 2001.

Wall, David S. *Cybercrime: The transformation of crime in the information age.* Cambridge: Polity Press, 2007.