

Research Needs for Computer Crime

Introduction

Between July and October 1995, the National Institute of Justice (NIJ) conducted an electronic conference on the subject of computer crime.¹ The purpose of the conference, which was called POLCOMP, was to identify basic and applied research needs on the growing problem of computer crime. The conference had 86 members with relevant knowledge and experience in investigation, prosecution, and training. It included a cross-section of skills and backgrounds, including law enforcement investigators, prosecutors, private investigators, academics, and many others. This report provides a summary of the substantive issues from the conference.²

Mr. Sam McQuade served as moderator for the POLCOMP electronic conference. In this role, he posed a series of questions to the group and guided the discussion as responses emerged. Starting with a basic inquiry on the definition of computer crime, POLCOMP participants moved into what is known about its prevalence, how police and prosecutors are addressing the problem, how current legislation impacts prosecution, and what the training needs are at the national and local level. Most importantly, conference participants made numerous suggestions for basic and applied research on these and related areas.

Electronic conferences provide a new forum for bringing a group of experts together to respond to questions and debate the direction of research in specified areas. The operation and conduct of an electronic conference has many parallels with moderated face-to-face meetings. As issues are presented, participants express their views and get reactions from others. The discussion sometimes

¹ The conference was conducted through a listserv established by the Institute for Law and Justice (ILJ). A listserv consists of a group of e-mail addresses that serve as an electronic mailing list. Each time someone sends a message to the group, it is automatically forwarded to everyone on the list.

² A separate report on the operation and conduct of listservs as an alternative to face-to-face conferences has been provided to NIJ.

gets heated as differences in opinion are expressed by participants, and a key role of the moderator is to control the discussion, interject summaries along the way and, as needed, referee disputes.

To develop this report on the substantive results of the electronic conference, a careful analysis of all messages was conducted to identify themes and trends among participants. It became clear early in the analysis that complete agreement on key issues would not be forthcoming. In part, this situation is due to the difficulties with electronic conferences to obtain a consensus on issues that are discussed and debated. While the moderator can control the debate, it is not possible with electronic conferences to ask for a show of hands on a conclusion.

In part, however, the lack of agreement gets to the very nature of computer crimes. As discussed in the next section, the term *computer crime* covers such a wide range of offenses that unanimity becomes an elusive goal. Participants reflected the variety. One participant was especially knowledgeable of hackers and their techniques for illegally breaking into computer systems. Another had expertise in offenses dealing with intellectual property. Others brought expertise in telecommunications crimes, frauds, counterfeiting, offenses against ATM machines, and many others. All these offenses fit under the rubric of computer crimes. The diversity of expertise compounded the difficulties of reaching consensus.

In spite of these problems, several important themes emerged as a result of analyzing the messages. First and foremost, computer crime is a serious problem in this country and world wide. Loss estimates range in the millions each year based on any of the several definitions of computer crimes available for choice. Moreover, computer crime is increasing each year, and the only debate among participants was the *rate* of growth. What is also clear from the conference is that, with a few notable exceptions, police and prosecutors across the country have not responded adequately to computer crimes. There is a lack of personnel, training, and equipment that pales in comparison to any other crime of similar magnitude. Indeed, some participants stated that one reason for the failure of businesses to report computer crimes is their belief that police and prosecutors may not understand the offense and, if understood, may not be able to react.

POLCOMP participants have a lot to say about the reasons for the current situation of continual increases in computer crimes, about the lack of attention by police and prosecutors, about the need for

extensive training, and about several other areas that need research attention. To them, the need for additional research is obvious, and their debates were on the priority and direction of the research. As the reader moves through the sections in this report, the complexities of computer crime and its investigations will become clearer, and it is anticipated that the need for research will be as evident as it is to these participants.

Definition of Computer Crime

At any conference, whether it is electronic or face to face, it is reasonable to start with defining the topic under discussion and proceeding from there with everyone on the same page. In POLCOMP, the first question posed by the facilitator followed this logical approach: “What is computer crime and how prevalent is it?” This seemingly innocuous question resulted in a dialogue among POLCOMP participants that lasted the better part of two months. They debated several definitions—some simple and others quite complex—in trying to reach a definition agreeable to everyone. On more than one occasion, a participant asked whether precise definitions were really important for the aims of the conference. The end result, as discussed later in this section, was a rather uncomfortable stalemate that approached the definition of computer crime in two different, but related, ways: legislative statutes and typologies by academicians.

The difficulties with definitions reflect more on the nature of computer crime than the knowledge base of conference participants. How does one develop a single, satisfactory definition of a crime that ranges from employees writing a letter on their work computer to the use of a computer for advancing the embezzlement of millions of dollar? The list of offenses has even greater dimensions, as reflected by examples of cases that POLCOMP participants have investigated that included fraud, pornography, theft, unauthorized modification of software, tax crimes, embezzlement, counterfeiting (driver’s licenses, stock certificates, birth certificates, car titles, checks, diplomas, and marriage certificates), unauthorized destruction of data, gambling offenses, credit card crimes, financial crimes, drug crimes, stealing telephone access codes, altering data (financial records, school grades, medical records, arrest records, court dispositions, and payroll deductions), and many others.

The variety of offenses under computer crimes also reflects the extent to which computers have entered our lives. As one POLCOMP participant stated,

Today, due partly to occupational migration and chiefly to computerization, we are more known by our digital identities than by our physical appearances. A digital identity is the information that is maintained in computers that defines and describes us to others. It may be a computer password, an ATM number, credit history, military record, the type of videos you rent or your mother's maiden name. A criminal can now assume another person's identity by using their digital identity, even though he doesn't physically resemble the person in any manner.

Other nuances of computer crimes compound the difficulties in defining computer crimes and legal sanctions. The fact that a computer file can be copied and transported to another system changes our concept of theft because the targeted item is not literally removed from where it resides. As another example, if a hacker breaks into a computer system and merely "looks around," a law has clearly been broken, but some view such offenses as minor, especially when the hacker takes nothing, makes no changes to the system, and notifies the system administrator about the security breach.

Finally, with the proliferation of microcomputers in business coupled with increased employees' knowledge base, most participants believe increases will occur in storage of personal information on a company's system (e.g., a spreadsheet for a personal checking account), e-mail communications to friends and relatives, and access to the World Wide Web system for information of personal interest (e.g., sports, cooking, music, opera, books, humor, etc.). While technically classified as misuses of computers, and perhaps even fraud through the company's access costs, most POLCOMP participants believe that it will be impossible to control these infractions. As one participant comments,

Employees have been writing letters on company typewriters and stealing stationery for decades. Because office tools have changed, are we to call the same behaviors high-tech crimes? The continuing thread is human behavior. Right from the start, we've got to be careful that we don't get bamboozled by techno-glitz terminology and high-tech crime hype into thinking that the tools of the information age are creating massive new waves of crime.

Problems with definitions become even more exasperated when digital identifies are coupled with the recent advances in telecommunications. These improvements over the last ten years now enable computers to link and talk to each other more efficiently, but this ease of communication is a two-edged sword because it creates opportunities for abuses. Many computer crimes are accomplished by someone sitting in the safety and security of their own home or business, without having to physically remove themselves to another premise, as with burglaries or robberies. The physical distance between offender and target computer may be hundreds or thousands of miles away, but the *electronic distance* is nothing.

Given this background, the following two subsections summarize the approaches to definitions provided by reviewing statutes and typologies for computer crimes.

State Computer Crime Statutes

Many POLCOMP participants made reference to state statutes as an approach to defining computer crime and as a strong influence on investigative and prosecutorial approaches. One participant offered the following breakdown as a way of thinking about definitions based on state and federal legislation:

For purposes of this response, it is assumed that "computer crime" means any illegal act, the commission of which (in whole or in part):

- A. targets computer hardware or software as a focal point of the act; or,
- B. utilizes computer hardware or software to accomplish or assist in accomplishing the act; or,
- C. involves or uses computer hardware or software to store, preserve, assimilate, or secrete any evidence or any fruits of the act; or,
- D. unlawfully accesses, invades or violates computer hardware or software integrity in accomplishing or in attempting to do the act.

From this perspective, the extent (quantitatively) of computer crime legislation is rather large. There are numerous federal and state statutes which can be used in the prosecution of computer crime. These statutes range from traditional crimes on the one hand (such as theft, fraud, criminal trespass, and embezzlement) to subject

direct statutes (such as the Counterfeit Access Device and Computer Fraud and Abuse Act) on the other hand.

To aid this discussion, ILJ posted a study conducted by Hugh Nugent in 1993 that summarizes the state statutes at that time in regard to computer crime. His report is in line with the above comments and provided further background on what constitutes computer crimes from a statutory viewpoint.

Every state has now enacted legislation on computer crime. Most have done so through a comprehensive statute, such as the state criminal code called the “Computer Crimes Act.”³ Others have inserted offenses, with appropriate definitions, into other statutes as in Ohio under its general theft statute coupled with an added section on denying access to a computer.⁴ California’s computer crime provisions, which appear under Crimes Against Property, is one of the most comprehensive and is updated every legislative session.⁵

Nugent summarizes the differences between the two approaches of state legislation:

With the comprehensive approach, the state legislature creates a new set of definitions and offenses, trying to face the broad array of potential criminal opportunities created by computer technology. There is always a fear that new definitions will give rise to new litigation as courts and litigants shake them down into accepted forms.

The other philosophy is to modify existing law by incorporating new concepts within established forms, thereby minimizing the potential for frustrating the legislative will. Established statutory definitions, approved jury instructions, and judicial precedents can be used. For example, if computer crime is viewed as a form of property crime, then the familiar concepts of property crime can be used in developing and defending cases. The impact of change is alleviated.

His analysis shows that most computer crime statutes provide definitions of terms, offenses, elements of offenses, and penalties, with some statutes containing additional provisions for venue, civil remedies, and affirmative defenses. The statute in Tennessee is considered to be a typical

³ E.g., *see* Alabama Computer Crime Act, Ala. Code §§ 13-A-8-100 through 103; Florida Computer Crimes Act, Fla. Stat. §§ 815.01 through 815.07; Illinois Computer Crime Prevention Law, Ill. Rev. Stat., ch. 38, §§ 16D-1 to 16D-7.

⁴ Ohio Rev. Code Ann. §§ 2901.01, 2913.81.

⁵ Cal. Penal Code, §§ 502, 502.01; *see also* §§ 1203.047, 2702.

comprehensive approach to legislative enactment about computer crimes. After a series of definitions, it defines a computer crime in the following manner:

- (a) Whoever knowingly, directly or indirectly, accesses, causes to be accessed, or attempts to access any computer software, computer program, data, computer, computer system, computer network, or any part thereof, for the purpose of obtaining money, property, or services for themselves or another by means of false or fraudulent pretenses, representations, or promises violates this subsection and is subject to the penalties of Section 39-14-105.
- (b) Whoever intentionally and without authorization, directly or indirectly
 - (1) Accesses, or
 - (2) Alters, damages, destroys, or attempts to damage or destroy any computer, computer system, or computer network, computer software, program or data violates this subsection.

For interested readers, the full report by Nugent is available through ILJ's Home Page, and Appendix A to this report contains Tennessee's statute.

The importance for computer crime investigations lies with the differences across states in the elements of offenses. As previously discussed, computer crimes have the unique characteristics of transcending physical distances, which means that investigators and prosecutors in different localities may have to cooperate to a high degree. An investigator in Los Angeles may need assistance in obtaining the records of a financial institution in Chicago or may need the assistance of a police department in Dallas to confiscate a computer system for review. The logistics in developing this cooperation are unparalleled with any other crime in requiring cooperating agencies to have the same legal and technical understanding of computer crimes. Given today's progress in computer crime investigations, cooperation is the exception rather than the rule.

Classification Systems of Computer Crimes

The other approach to defining computer crimes is to develop a classification scheme that links offenses with similar characteristics into appropriate groups. Several schemes have been developed over the years. As a broad classification, one POLCOMP participant suggested two general

categories: *active* and *passive* computer crimes. An active crime is when someone uses a computer to commit the crime, such as when a person obtains access to a secured computer environment or a telecommunications device without authorization (hacking and phreaking). A passive computer crime occurs when someone uses a computer to both support and advance an illegal activity. An example is when a narcotics suspect uses a computer to track drug shipments and profits.

Expanding on these two categories, this participant stated,

While both types of crimes are on the rise, active crimes have been around longer and are growing at a much faster rate....Passive computer crimes are the newest crime that is starting to plague law enforcement. Passive computer crimes are certainly on the rise and at a good pace. More and more criminals are taking advantage of the user friendly aspect of the computer and the technological advancements of high technology to help in the commission of their crimes or to even support and further their crimes.

Today, criminals can print money with color printers and easy-to-use publishing programs, they can clone phones with cloning software that is available for free on underground bulletin boards, they can manage their illegal business with a variety of popular business software and they can protect their illegal activities from the prying eyes of law enforcement by the use of FREE encryption programs. These are only a few of the hundreds of possibilities that computers can be utilized by the criminal community. Remember, criminals don't have to be computer literate as computers are so friendly today.

Let me sum up by saying that I have worked a variety of both active and passive computer related crimes. These include homicide, corporate computer intrusions, governmental computer intrusions, terrorist bombings, credit card fraud, hacking, phreaking, organized crimes and sex crimes. No matter what type of crime is being committed, the chances that a computer could be involved in the crime either as a tool or as evidence is growing at a rapid rate....In my opinion, these crimes will grow at a rate greater than the rate of people buying a computer for the first time.

In line with the active and passive approach, another participant noted,

In analyzing the [computer] crime problem, I think it is important to distinguish between cases where computers are targeted (that is, the

actor's conduct is designed to cause damage to, or steal information from, a computer system) and those cases where computers are used as tool to facilitate some traditional offense (embezzlement). We also need to distinguish between outsiders and insiders, since they present separate problems for law enforcement and victims.

POLCOMP participants also made reference to other classifications of computer crimes that have appeared in a variety of publications from academicians and other interested parties in the field. As an example of a recent publication, Carter (1995) puts forth four general types of computer crimes:

- Computer as the Target—theft of intellectual property, theft of marketing information (e.g., customer lists, pricing data, or marketing plans), blackmail based on information gained from computerized files (e.g., medical information, personal history, or sexual preference).
- Computer as the Instrumentality of the Crime—fraudulent use of automated teller machine (ATM) cards and accounts; theft of money from accrual, conversion, or transfer accounts; credit card fraud; fraud from computer transactions (stock transfers, sales, or billings); and telecommunications fraud.
- Computer is Incidental to Other Crimes—money laundering and unlawful banking transactions, BBSs supporting unlawful activity, organized crime records or books, and bookmaking.⁶
- Crimes Associated With the Prevalence of Computer—Software piracy/counterfeiting, copyright violation of computer programs, counterfeit equipment, black market computer equipment and programs, and theft of technological equipment.

The difficulties of the POLCOMP participants in reaching agreement on the definition of computer crime had an impact throughout the remainder of the conference. The primary difficulty was in trying to make global statements about computer crimes. Any attempts in this direction had major exceptions. Other difficulties were encountered in discussions on training needs for computer crimes and, of course, in shaping the direction of future research. As reflected in the last section of this report, the needs for research are extensive in part because of what constitutes computer crime.

⁶ Carter cites one case in which a suspect committed murder by changing a patient's medication information and dosage in a hospital computer.

The following section discusses the prevalence of computer crimes based on available snapshots that have been developed by interested parties. Subsequent sections discuss the needs in the legislative and training areas, and the report concludes with a section on research needs.

Prevalence of Computer Crimes

As reflected by POLCOMP participants, the correct answer to the amount of computer crime is “nobody knows, but there’s a lot.” Given the discussion in the last section on definitions, an ambiguous answer should come as no surprise. If there is no satisfactory definition, then estimates of overall prevalence are baseless. On the other hand, occasional efforts have been made to estimate specific types of computer crimes, and these estimates, as discussed below, clearly indicate huge economic losses.

Putting aside the problems surrounding definitions, POLCOMP participants offered several other reasons for why reliable statistics about the total amount of computer crime are unavailable:

- Computer crimes may go undetected, as when someone breaks into a computer, copies files, and then leaves without detection by the system or its operators.
- Computer crimes may not reported to police or prosecutors.
- The Uniform Crime Report system does not include classifications for computer crimes and no other national system exists for collecting statistics about the problem.
- Arrests are not a reliable source for computer crimes because the charges may be placed under an unrelated statute, especially when the computer has advanced a crime, as in embezzlements.

The information available about the extent of computer crimes, mostly from telecommunication businesses and associations, offers an eye-opening picture of economic losses. As reported by POLCOMP participants, some of the figures are:

- Active computer crimes are responsible for what is now estimated to be over five billion dollars per year in losses to the high-tech industry.
- According to the Network and Telcom Security Review, a respected industry newsletter, losses for telecommunications will reach \$3.375 billion for 1995 nationwide. This figure is for phreaking (stealing phone services) only; it does not include cellular fraud or hacking.

- An article from a San Francisco newspaper (July 18, 1995) states that a United Kingdom survey of 1,000 organizations showed a rise in all forms of cyberspace illegality, including a 183 percent rise in the average cost of reported incidents.
- Annual losses from corporate telephone systems (called PBXs) attacks alone may amount to over \$500 million.

One participant made a comment about the international picture, and while not containing dollar figures, it shows the widespread nature of the problem:

In general, I can respond in relation to computer crime as it is occurring—and has occurred since the mid-1960s—in Australia, Europe, South East Asia, the Middle East and, to some extent, in Africa...Computer-related crime is rife in these regions. Further, developed countries (i.e., United States, United Kingdom, Canada, Australia, etc.) are often seen to be targeted by people in developing countries. So is the capitalist world, in general, where there are more computers per head of population, etc. Various viruses have come from behind (what was) the Iron Curtain. Locally, mainland China (and Southeast Asia generally) proves to be a major source of pirate software which is distributed to worldwide markets.

As local flavor, one POLCOMP participant is an police officer in a town of 60,000 population who, along with another officer, has investigated computer crimes on an “as needed” basis during the past five years. He commented that “computer crimes are prevalent and computer criminals operate with relative impunity.” A sampling of his cases follows:

- Case 1. Suspect uses computer to “war dial” local phone numbers, suspect’s computer identifies a PBX machine access port, suspect hacks into PBX machine, suspect posts PBX access code on private BBSs. Over \$100,000 in unauthorized phone charges are incurred by the victim company.
- Case 2. Suspect uses computer to make unauthorized access to telephone company computer and obtains list of “trapped” lines.
- Case 3. Suspect uses computer to access a community college computer network. Community college incurs over \$20,000 in expenses to evaluate the authorized access and determine if suspect planted a virus.
- Case 4. Suspect modifies TV satellite receivers so receivers can be programmed with wizard codes. Wizard codes enable receiver to fraudulently obtain pay-per-view and

pay-for-view satellite transmissions. Suspect operates a BBS so his customers can call in and obtain monthly wizard codes.

- Case 5. Suspect is a convicted child molester on parole. Suspect operates a BBS which minors frequent. Suspect obtains personal information on juveniles when juveniles apply for access on BBS.
- Case 6. Suspect uses computer equipment to produce counterfeit currency and checks.
- Case 7. Suspects operate computer BBS to traffic in illegal information: long distance calling card numbers, credit card numbers, voice mail accounts and passwords, computer system accounts/passwords.
- Case 8. Suspect hacks into high school computer, accesses teacher accounts, destroys and alters data.

He also notes that arrested suspects have posted detailed reports and recommendations to others regarding how to avoid arrest and, if arrested, what to do. The network is effectively a “computer gang” with common interests in illegal activities with computers. The public generally does not hear about the types of cases described above because the usual reporting is on the large, sensational computer crime. As one participant noted, “The news media has hyped the topic of computer crime to unrealistic levels.”

A final theme of interest from POLCOMP participants centers on the future direction of computer crimes due to increased numbers of computers, continued improvements in telecommunications, and growth of the World Wide Web under Internet. Several POLCOMP participants believe that increases in computer crime will track with these trends. One participant puts the issue this way, “I suspect that a respectable barometer of the prevalence of the use of computers in crime quite possibly and reasonably parallels their use in industry, business, and home. If that is, in fact, the case, then computer crimes certainly appear to be of epidemic proportions.”

Legislative Needs

POLCOMP participants identified two related problems with current legislation, at the federal and state level, that impact on investigations and prosecutions of computer crime:

- Weaknesses in the provisions and application of selected federal and state statutes.

- Slowness of legislators to react to new computer crimes.

The lament of several participants is that major cases have surfaced over the past few years in which defendants were found not guilty because present laws did not adequately cover the offense. An example at the time of the conference was the arrest by a U.S. Attorney's Office of Mr. David La Macchia, a student at the Massachusetts Institute of Technology, who ran a bulletin board in which he allegedly gave away over one million dollars worth of copyrighted software. Mr. La Macchia would allow users of his bulletin board to download any of the software on his system to their system at no cost. He was found not guilty because the relevant statute stated that economic gain had to be established. At least one POLCOMP participant believed that the facts of the case should have resulted in a conviction for the transfer of stolen property or a violation of copyright laws.

At the state level, as noted in Nugent's report, a clear legislative problem is that different states have vastly different definitions of what constitutes a computer crime. There is no consistency, except in a few states that have basically copied each other for their statutes. The analysis by Mr. Nugent raises the question of whether it is feasible for all states to have a uniform computer crime statute.

The second problem, as identified by POLCOMP participants, is the lag between technological advances and legislative action. As noted by one participant,

Computer crime legislation is now and has been for a good period of time, behind the times. Its effectiveness as a tool for law enforcement to help combat high technology related crimes has been greatly diminished. The legislative process is in and of itself the crux of the problem. By its very nature, the legislative process is a long and arduous process by which laws are created. The problem is that technology changes so rapidly that the laws which were proposed over a year ago and that are voted on today, are already behind the times. That is even before they actually become law.

Crimes dealing with intellectual property are the main example given of new offenses that need to be addressed by legislation.

The research problem emerging from these comments is the development of a process for more rapid legislative reaction to technological advances. As stated by another participant,

In the past, society would adjust to change, usually at the same rate of that change. Today, this is no longer true. The information age has ushered in dramatic technological changes and achievements, which continue to evolve at geometric rates. The creation, the computer itself, is being used to create new technologies or advance existing ones. This cycle means that changes in technology will continue to occur at an ever increasing pace. What does this mean to the system of law? It means we have to take a look at how we establish our system of laws. We must adapt the process to account for the rate of change.

Training Needs

POLCOMP participants provided more comments about training needs and problems than any other topic. They were virtually unanimous on the need for training, but differed significantly on who should be trained, what the training curricula should be, and how training should be conducted. Another problem discussed by the group centers on the experiences of police personnel and prosecutors after they received specialized training. Several participants commented on the lack of appreciation within agencies for the skills of these personnel.

With regard to the need for training, participants noted both the lack of *general* training about computers in local police departments and *specific* training for computer crime investigators. As one participant stated,

Training seems to have always suffered the most in law enforcement agencies, and with regard to computer and technology training, the gap is even wider. Most experienced cops today suffer from a total lack of contact with available technology and simply don't have the time to learn....I don't think agencies have a choice for future training. It has to be done or we will continue to fall further behind the mainstream public and criminals in the recognition and utilization of technology.

Another participant noted the paradox between the continued acquisition of computer technology by many police departments and the lack of computer literacy by police employees:

While the number of law enforcement agencies utilizing computers to investigate crimes is rising at a good rate, the number of law enforcement officers becoming computer literate and subsequently utilizing computer technology to become more efficient is growing at a much slower pace. Agencies can become more efficient and produce greater investigative output by getting their officers involved with technology. By the use of training and subsequent interaction with computer technology, officers will soon become comfortable with technology and start to produce results that are possible only with the use of technology.

Other participants tied the lack of computer literacy in many police departments to reluctance by corporations to report computer crimes. The experiences of an investigator in POLCOMP typifies this problem,

I frequently get calls regarding computer crime questions and many of the questions deal with corporate computer concerns, e.g., theft of trade secrets, improper use of equipment by employees, decryption problems, etc. My logical question back to them is why don't you go to the police. Their typical response is that the police in their area don't understand computer technology issues.

In other words, the police must learn to "talk the talk" before corporations will be willing to discuss sensitive issues, such as trade secrets and damaging computer crimes. Failure to appreciate the severity of this problems will result in an ever-widening gap between police and victims of these crimes with corporations viewing the police as inept in understanding computer technology and seeking help elsewhere with their problems. The difficulty with this approach is that the perpetrator may be found out and forced to leave the corporation, only to get a job elsewhere and commit the same offenses.

While recognizing the need for training, the group debated who should receive training and how the training should be delivered. Should all officers in a department receive training or only a selected number of officers? How much training is needed and on what topics? What are the advantages and disadvantages of the variety of potential training delivery systems, including a centralized location, regional centers, courses in community colleges, videotapes, and networked computers? There were almost as many opinions as members of the conference. The discussion surrounding the issues illustrates

the variety of potential approaches, but also highlights the problem that consensus on training may occur only with additional research on the topic.

Several participants noted that not every police and prosecutor staff needs a computer crime expert, but there is a need for all employees to recognize a potential computer crime, understand what to do at the scene, and have an expert available when needed. As noted by a participant,

First, every agency must be able to anticipate when a computer might be involved in a case so its personnel can anticipate the situation, even if its actual appearance is unexpected. Second, every agency must become familiar with the state and federal statutes and case law which affect the substantive and procedural aspects of computer crime. State computer crime laws, the ECPA, the PPA, and state and federal search and seizure constitutional law decisions are the starting point. Third, add to that sufficient technical competence to secure a system on site or transport it back to headquarters. Fourth, if all needed expertise is not on staff, know where to get it.

As an “immediate and first step,” one participant saw the need for training all police officers and prosecutors with three basic courses: (1) an introduction to computer evidence awareness, (2) identification, collection, transportation and preservation of electronic evidence and related components; and (3) where to find an expert data recovery specialist. Another participant, with 16 years of prior experience in a sheriff’s agency, teaches a community college course on computers and computer crime with a wide-ranging curriculum that includes:

- Introduction to computer operations
- Operating systems
- Windows operating system
- Data collection and organization
- Database design
- Statistical analysis of gathered data
- Inter-connectivity
- Computer aided dispatch systems
- Information management
- Knowledge based systems
- Methodology of investigation
- Examination of floppy disk
- Computers as a crime tool
- Computers related to a crime
- Data protection and encryption
- Seizing a computer system

The curriculum highlights the range of knowledge and skills required for these investigations starting with a basic understanding of computers and extending to the more difficult topics of communications and data protection.

Supporting the need for training a wide police audience, one of the investigators of high technology crimes offered the following view,

Law enforcement investigators as a whole need to have training in computer related crimes. Child abuse/exploitation investigators need to know that molesters are using computer-to-computer interaction to identify, contact, and exploit children. Computer-to-computer connections are aiding in the possession and exchange of child pornography. Burglary/larceny investigators need training in computer theft, computer component theft and the gray market. Forgery/fraud investigators need training since computer criminals frequently engage in fraudulent activities. Various other types of investigators need to recognize that a computer in a suspect's home may hold vital evidence which relates to the type of criminal activity they are investigating.

Compounding the need for training are the experiences of what happens within the police agencies after the training occurs. As described by POLCOMP participants, the result all too often is that the agencies do not appreciate the skills of employees trained in computer technologies, as reflected by the following comment,

There is a major problem with offering anyone computer training if they are working in the context of an organization which has not itself come to terms with the use of high technology. A cop—any cop—is hamstrung by an administration which is more likely to slap him on the wrist for innovating. We have various cases on file—from worldwide locations—of cops' promotions being curtailed by their becoming technonerd.

The problem, as expressed by other participants, is that law enforcement managers fail to tie computer evidence and related computer investigations to traditional investigative methods and procedures with the result that computer investigations are secondary in terms of priorities for investigation, funding requirements, and promotional opportunities.

Considerable disagreement arose over whether training should be centralized through the establishment of a federally sponsored center. Such a center is already underway under the direction of Mr. Bill Spernow, a participant in the conference. Appendix B contains a detailed explanation of the

National Investigative Computer Forensic Assistance Center provided by Mr. Spernow during the conference for comment by the group.

In the ideal world, with considerable financial wealth, it would clearly be advisable to have several training vehicles to serve the variety of needs at the federal, state, and local level. A well-financed national training center has the advantage of offering specialized expertise and training for a crime that frequently demands several skills and constant upgrading of these skills. On the other hand, as noted by several participants, centralized training may not be cost effective and local agencies cannot send large numbers of their personnel away for training. Local training is certainly preferable when the objective is to convey basic information to all officers, investigators, and prosecutors about aspects of computer crime. The difficulty is the variation in the quality of local training and the lack of universal standards on topics to be taught.

As one solution to the above problems, POLCOMP participants suggested the development of a “virtual reality university” which would provide training through a nationwide communication network. A specific suggestion by a participant ran as follows,

My suggestion is that NIJ should fund the research, development and creation of a law enforcement "virtual reality university". This would include implementation of the concept and continued and on-going support of the university itself once it is established.

This university could be a Virtual Reality University for Law Enforcement (VRTULE) which contained core curriculum for technological law enforcement training. The University could be accredited, leading to recognized degrees for officers, and consist (among other things) of distance-learning and dispersed faculty and students throughout the United States (if not the world).

A core curriculum would have to be developed; protocol would have to be established, entrance requirements (and security issues) would have to be addressed. Residency requirements could be established similar to means used by other universities which have gone on-line to offer hi-tech courses.

Is there a better way to train, develop and educate high technology law enforcement officers than through VRTULE - which would include competency based, hands-on instruction?

Research Needs

Toward the end of the conference, participants were asked to provide their ideas for potential NIJ-funded research in computer crime. In responding to this request, the participants touched on all the topics discussed in the above sections. For purposes of presentation, we have divided the suggestions into the categories of *basic research* and *applied research*. The resulting lists are extensive, but not exhaustive, in covering the research needs.

Basic Research

General

- Identify the trends in computer hardware, software, telecommunications, and cyberspace that will impact the extent and severity of computer crime over the next 25 years.
- Determine the role of police and prosecutors in the regulation of cyberspace.
- Review the impact of encryption programs on computer crimes and investigations.
- Determine ways to create a focus on computer crime as a national and local priority.

Classification of Computer Crime

- Develop standard definitions for computer crimes.
- Develop a standardized system for reporting computer crimes for national statistics.

Legislation

- Examine the feasibility of uniform computer crime statutes for the states.
- Determine whether adaptations can be made to the legislative processes for faster responses to technological advances.

Investigation

- Develop uniform standards for gathering computer evidence.
- Develop forensic software to assist computer crime investigations.
- Determine the impact of the Telecommunications Act on computer crime investigations, especially in regard to distribution of pornography.

Training

- Determine the roles of centralized, regional, and local training.
- Determine the role of college courses, including community colleges, in computer crime training.
- Establish basic and advanced curricula for computer crime training.
- Determine the feasibility of a Virtual Reality University for Law Enforcement to provide training on computer crime investigation and prosecution.

Applied Research

Extent of Computer Crime

Hackers, phreakers, crackers

- Estimate the true cost of computer intruders to businesses and individuals.
- Determine the percent of attacks that cause damage to the victim's computer (e.g., operations disrupted, data lost, etc.).
- Determine the percent of intruders who use Internet, as opposed to dial-up lines, for attacks.
- Determine the percent of attacks that result in theft of data.
- Determine the percent of victims who call police and Determine the percent that are repeat victimizations.
- Determine the percent of victims who are repeat victimizations.
- Determine the percent of victims call police.
- Determine the percent of intruders are arrested and convicted.

Techno-crimes

The effort here on the extent of these crimes depends on acceptable definitions of computer crime as determined by prior research. It could include financial fraud, counterfeiting with computer technologies, transmission of pornography, fraudulent use of ATM cards, fraud from computer transactions, illegal uses of cellular phones, and many others. With each type of offense, the aim is to

estimate the extent of the offense and the success of the police and prosecutors in combating them.

Law Enforcement's Response to Computer Crimes

Federal efforts

- Review federal agencies with responsibilities for computer crime investigation and prosecutions.
- Determine extent of overlapping responsibilities.
- Determine whether a separate federal agency should be established for crimes involving the use of the Internet or cyberspace generally.

Local efforts

- Establish coordination between public and private investigators for more effective investigations of computer crimes.
- Establish coordination between professional associations for more effective investigations of computer crimes.
- Establish a private listserv for communication between federal, state, local, private and academic arenas.
- Develop software to assist local agencies in investigation of computer crimes.

Training

- Establish a clearing house for computer crime investigations to include books, texts of statutes, newsletter, CD-ROMs, videos, etc.
- Establish a “virtual reality university” for training police and prosecutors as an accredited entity with opportunities for degrees.

Conclusions

Perusal of these research issues should raise at least two reactions on the part of readers of this report. First, as reflected unceasingly by conference participants, the most basic information on computer crimes is lacking in this country. The refrain by participants that “we don’t know how much there is, but it’s a lot” certainly reflects their individual experiences, but does little to raise the national consciousness on the subject and offers no insight into next steps. Second, the scope of research on

computer crime is very wide. Research plans may need to start with determining what aspects of computer crime are most important and most amenable to research.

Other technological advances occurring worldwide also impact any discussion of computer crime and the research that should be done. These advances include rapid expansion of the Internet with its World Wide Web (WWW), continued improvements in telecommunications, readily available encryption programs, and many others. We are therefore required to consider other issues—privacy, freedom of speech, and ethical behavior—that will impact as a moral collective on what is decided for the research parameters. The technological changes in this so-called *cyberspace* or *virtual community* are taking place with such rapidity that even the idea of policing the community is open to question. Any new technology creates a need for a community to determine what the norms of behavior should be for the technology and how these norms should be reflected, if at all, in our laws. With regard to cyberspace issues, we are at the stage of determining what the norms should be.

REFERENCES

Carter, David L. July 1995. "Computer Crime Categories." *Law Enforcement Bulletin*. U. S. Department of Justice: Federal Bureau of Investigation. 64(7), p. 21-26.

Hollinger, Richard C., and Lonn Lanza-Kaduce. "The Process of Criminalization: The Case of Computer Crime Laws." *Criminology*. 26(101).

Nugent, Hugh. *State Computer Crime Statutes*. 1993. Washington, D.C.: National Institute of Justice.

Appendix A. Tennessee's Statute on Computer Crime.