U.S. Department of Justice
Office of Justice Programs
National Institute of Justice

National Institute of Justice

Research in Brief

Julie E. Samuels, Acting Director

August 2000

State and Local Law Enforcement Needs to Combat Electronic Crime

By Hollis Stambaugh, David Beaupre, Dr. David J. Icove, Richard Baker, Wayne Cassaday, and Wayne P. Williams

Issues and Findings

Discussed in this Brief: The National Institute of Justice (NIJ), at the request of the National Cybercrime Training Partnership (NCTP), sponsored a series of workshops with State and local law enforcement agencies nationwide to ascertain their needs for combating electronic crime. The following project synopsis is derived from a full report that NIJ plans to make available in fall 2000. The full report presents the complete results of the research and analysis, inviting a response to the critical needs profiled in this document.

Key issues: A compelling need exists to better address the requirements of State and local law enforcement agencies in detecting, investigating, and prosecuting individuals who commit electronic crimes.

For the purposes of this study, electronic crimes included a spectrum of offenses ranging from fraud, theft, forgery, child pornography, cyberstalking, industrial espionage, and computer intrusions, as well as any other offenses that occur in an electronic environment. Also addressed in the study is a component of electronic crime—cyberterrorism—a premeditated, politically motivated attack against information systems with the

continued…

U.S. Attorney General Janet Reno recently said, "Whether it [technology] benefits us or injures us depends almost entirely on the fingers on the keyboard. So while the Information Age holds great promise, it falls in part upon law enforcement to ensure that users of networks do not become victims of New Age crime."

The rapid proliferation of computer systems, telecommunications networks, and other related technologies—upon which virtually everyone relies—presents concomitant widespread vulnerabilities. Increasingly, criminals are abandoning their guns for sophisticated computer-assisted weapons. Recent acts of electronic crime in the United States, such as the $15 million white-collar case dubbed "Operation Derailed" in Atlanta, Georgia, demonstrate the need for increased vigilance by law enforcement.[1] The highly publicized "Melissa Virus" and "Solar Sunrise" cases further exemplify how reliance on the Internet and electronic correspondence has subsequently increased vulnerability to cybercrime.

The statistics and losses remain staggering, and law enforcement agencies must be able to detect, investigate, and prosecute these cases. A recent report on cybercrime by the Center for Strategic and International Studies (CSIS) says, "almost all Fortune 500 corporations have been penetrated electronically by cybercriminals. The Federal Bureau of Investigation (FBI) estimates that electronic crimes are running about $10 billion a year but only 17 percent of the companies victimized report these losses to law enforcement agencies." In addition, a 1999 survey conducted by the Computer Security Institute (CSI) and the FBI of 521 financial institutions, universities, government agencies, and corporations found that 62 percent reported intrusions.

Of particular concern is the gap between training and technologies available to and used by law enforcement—especially State and local agencies—and the advanced technologies used by persons and groups committing electronic crimes.[2]

Assessment of State and local law enforcement needs to combat electronic crime

In fall 1998, the National Institute of Justice (NIJ) funded a 1-year study to identify, document, and respond to shortfalls in State and local law enforcement capabilities and resources for addressing electronic crime. This study built upon a January 1998 report by the National

Issues and Findings

continued…

intent to disrupt the political, social, or physical infrastructure of a target.

Key findings: State and local participants in the project provided researchers with a firsthand account of the technology tools required by law enforcement agencies to combat electronic crime. They also described the trends in cybercrime within their jurisdictions. On the basis of participants' statements, researchers made the following observations:

- There is a near-term window of opportunity for law enforcement to gain a foothold in containing electronic crimes, which presently outpace most agency investigative resources.

- Most State and local law enforcement agencies report that they lack adequate training, equipment, and staff to meet their present and future needs to combat electronic crimes.

- Greater awareness of electronic crime should be promoted for all stakeholders, including prosecutors, judges, academia, industry, and the general public.

Target audience: State and local policymakers; law enforcement officers and administrators; prosecutors and judges; State and national training centers; academia, industry, computer engineering, and security development specialists.

Cybercrime Training Partnership (NCTP) that sought input from 35 police chiefs across the Nation about the status of electronic crime and what training and technical assistance would be of greatest value to them.[3]

Discussed in this Brief are the results of a representative national inventory of State and local law enforcement agencies, conducted to determine the technologies, policies, and collateral support needed to combat electronic crime.

Methodology

In fall 1998, NIJ designated a management team to oversee the project's day-to-day operations. The team consisted of representatives from the TriData Corporation, U.S. Tennessee Valley Authority Police, U.S. Navy Space and Naval Warfare Systems Command, and U.S. Department of Justice (DOJ).

The team held a kickoff meeting to develop the assessment instrument and construct a strategy to implement the study. The assessment instrument, or protocol, was designed by the project management team and reviewed by subject matter experts, investigators, prosecutors, and training specialists. Groups that contributed to this effort included NCTP members, workshop facilitators, and other subject matter experts. The protocol was divided into the following sections:

- State and local perspectives on electronic crime.
- Profile of electronic crimes and investigation needs.
- Legal issues and prosecution.
- System vulnerability, critical infrastructure, and cyberterrorism.
- Forensic evidence collection and analysis.
- Training.

The management team, with assistance from five regional offices of NIJ's National Law Enforcement and Corrections Technology Center system and NCTP, selected potential participants. Care was taken to ensure that law enforcement disciplines specifically relevant to electronic crime efforts (such as investigation, search, seizure, forensic examination of electronic media, and unit management) were represented.

A total of 126 individuals representing 114 agencies participated in this national inventory. They represented a variety of urban and rural jurisdictions and a broad segment of State and local law enforcement entities, including sheriffs' departments, city police, State bureaus of investigation, crime laboratories, transit police, and regulatory agencies.

The agencies and their representatives were selected on the basis of their particular role in combating electronic crime. In addition, researchers interviewed electronic crime experts to gain insight and obtain advice on research design. Researchers also reviewed relevant literature to derive additional background information on tactics, techniques, and technologies currently available.

In the sessions, facilitators asked participants to identify the training, investigative support, and technology capabilities they needed to combat electronic crimes. They were also asked to describe typical offenders and their targets, most prevalent types of cases, and recently observed trends in electronic crimes.

After concluding the workshops in March 1999, members of the project management team analyzed, documented, and charted the inventory results. They identified significant findings, arrived at general conclusions, and made specific recommendations. During several iterations, the entire management team—along with workshop facilitators and subject matter experts—reviewed the final report for completeness and accuracy.

Findings and conclusions

The State and local law enforcement participants in this assessment provided a firsthand perspective of the technology, policies, research, training, and direct assistance required to combat electronic crime. Participants related their experiences with electronic crime and their concerns for the future, thereby providing a wealth of information for government decisionmakers in both policy and program arenas.

The participants identified dozens of needs across the spectrum of electronic crime. These needs were documented, categorized, and evaluated. Ten areas of concern, identified as the "Critical Ten," dominated the discussions along with commentary on what the future could hold for addressing each need.

In addition to these priority needs, two overarching issues emerged. Whether the need is high-end computer forensic training or onsite task force development assistance, progress must be accomplished quickly and in a centralized, coordinated manner.

Why the sense of urgency and the focus on coordination? The window of opportunity for law enforcement to keep pace with electronic crime offenders (let alone get ahead of the problem) is quite short. The capacity of technology used by these offenders is increasing geometrically and at a pace that significantly challenges public-sector resources at the State and local levels.

The emphasis on a coordinated approach is both practical and logical, as there is little time and few resources available to address this increasingly significant problem. The greatest impact will be generated if near-term solutions can be crafted and delivered through existing structures that have a broad reach and include most key stakeholders.

- The most important aspect of these challenges is the time sensitivity. Unless a national effort is launched in the near term, electronic crimes will outpace the resources of most State and local law enforcement agencies.
- There is a need to maximize investments in new or expanded tools, training, onsite assistance, and research with regard to electronic crime and cyberterrorism initiatives.

Critical Ten priority needs

From the assessment study, workshop participants determined 10 top priority needs. They are listed below, without reference to priority or ranking:

Public awareness. A solid information and awareness program is needed to educate the general public, elected and appointed officials, the criminal justice community, and the private sector about the incidence and impact of electronic crimes.

With many cases being undetected or unreported, and with the dearth of hard data on electronic crime trends, most individuals are unaware of the extent to which their financial status, businesses, families, or privacy might be affected by electronic crime. Neither are most people aware of how quickly the threat is growing.

A multifaceted information and awareness campaign is needed to clearly document and publicize how electronic crimes affect society. Unless the public is made aware of the shift in crime to the whole new arena of the Internet, individuals will continue to be subject to a number of crimes, including fraud, identity theft, child abuse, and denial of services.

Data and reporting. More comprehensive data are needed to establish a clearer picture of the extent and impact of electronic crime and to monitor trends.

In response to the Computer Fraud and Abuse Act, the FBI amended its Uniform Crime Reporting System to address electronic crime. The FBI placed a question within its National Incident Based Reporting System to document if a criminal offender used a computer in the commission of the crime.

However, additional details about the use of computers in crime are needed to fully measure the incidence of electronic crime.

Without more data, detailed analysis, or a crime victimization study, it is difficult to track regional or national trends in electronic crime. Hard data are needed both to better understand the era of electronic crime and to communicate it to budget and policymakers, as well as to citizens.

Uniform training and certification courses. Law enforcement officers and forensic scientists need specific levels of training and certification to correctly carry out their respective roles when investigating electronic crimes, collecting and examining evidence, and providing courtroom testimony.

This training should reflect State and local priorities. There is a need for both entry-level and advanced training for law enforcement officers and investigators, prosecutors and defense attorneys, probation and parole officers, and judges.

First-line officers who secure the initial crime scenes need training on basic forensic evidence recognition and collection techniques. National guidelines should be developed and applied toward a certification program that ensures uniform skill levels. Additionally, prosecutors and judges need awareness training to stay abreast of electronic crime's impact and technology.

Management assistance for onsite electronic crime task forces. State and local law enforcement agencies need immediate assistance in developing computer investigation units, creating regional computer forensics capabilities, organizing task forces, and establishing programs with private industry.

A majority of the agencies represented in this study called for a county (or regional) investigative task force approach to the technically challenging and time-consuming job of investigating crimes involving computers. Agencies are seeking hands-on assistance from experts in electronic crime and in criminal task force development to enhance their ability to combat electronic crime at all levels.

Simply stated, investigative task forces are extremely effective crime-fighting tools. This has been proven with drug and arson task forces.[4] Combining forces among agencies makes it more affordable to acquire the high-tech tools used in analyzing computer evidence and to coordinate strategies and procedures to deal with electronic crime.

Direct assistance in forming electronic crime task forces is urgently needed for several reasons. Specially trained personnel and dedicated forensic laboratory equipment are often required to examine and retrieve evidence that is necessary for prosecution and contained in a computer's hard drive.

Electronic evidence often implicates individuals from jurisdictions where officials' testimony and involvement in case proceedings must be coordinated. Also, for many prosecutors, presenting high-tech evidence in court is challenging, in terms of both ferreting through highly technical terms and making them understandable for a jury.

Updated laws. Effective, uniform laws and regulations that keep pace with electronic crime need to be promulgated and applied at the Federal and State levels.

Over the past decade, use of computers and the Internet has grown exponentially, with individuals becoming more dependent on these technologies on a daily basis. As computer use has blossomed, so too has criminal involvement. Deterring and punishing these offenders requires a legal structure that will support early detection and successful prosecutions. Examples of emerging trends include the increased reliance of criminals and terrorists on encryption technologies and obvious efforts to cloak the identity and location of offenders.

Currently, there is no formal legal mechanism to require that subpoenas generated in one State be enforced in another. There is a practice of cooperation, in which one State attorney general's office voluntarily assists another State authority in either serving an out-of-State subpoena or seeking an in-State court order to enforce the out-of-State subpoena. However, the reliability and consistency of this procedure are not uniform, and the ability to secure enforcement of an out-of-State subpoena on a recalcitrant party is at best questionable.

Clearly, the laws defining computer offenses, as well as the legal methods needed to properly investigate current electronic crimes, have lagged behind technological and social changes.

Cooperation with the high-tech industry. Crime solvers need the industry's full support and cooperation to control electronic crime.

Industry support is needed to develop and maintain trusted relationships and cooperative agreements to help sponsor training, join task forces, and share equipment for the examination of electronic evidence. These cooperative relationships can also encourage the reporting of electronic crime.

Michael A. Vatis, Director of the National Infrastructure Protection Center, FBI headquarters, Washington, D.C., recently commented on a joint CSI and FBI annual study that assessed the levels and costs associated with computer crime.

Vatis stated, "This year's CSI/FBI study confirms the need for industry and government to work together to address the growing problem of computer intrusions and cybercrime generally. Only by sharing information about incidents, and threats, and exploited vulnerabilities can we begin to stem the rising tide of illegal activity on networks and protect our nation's critical infrastructure from destructive cyber attacks."[5]

Many technology firms have their own information security units that, among other responsibilities, detect and investigate electronic crime. Increased cooperation between industry and government provides the best opportunity to control electronic crime and protect the Nation's critical infrastructure, which heavily relies upon computer technology.

Special research and publications. Investigators, forensic laboratory specialists, and prosecutors need a comprehensive directory of electronic crime information, training, and resources to help them combat electronic crime.

The Federal Government, State governments, colleges and universities, trade associations, and private industry are all responding to the need for diverse training in the field of electronic crime. It is critical to communicate the availability of training and professional seminars if these offerings are to be used to their maximum advantage.

Many investigators and prosecutors are calling for a clearinghouse of online information and technical guidance on methods, investigative technologies, and research. Examples of specialized technologies include the ability to detect and break encryption, image disks, and index important information.

State and local law enforcement agencies also are asking for a clearinghouse of national and State experts and resources. A "who's who" of electronic crime investigators, unit managers, prosecutors, labs, equipment, expert witnesses, and so forth would be a well-received guidebook for many practitioners who frequently noted the need for information on how to contact colleagues in other communities. A training directory citing current sources of electronic crime training offerings (print, online, and CD-ROM versions) would be extremely valuable.

One such successful nationwide law enforcement network, which supports the dissemination of information on electronic crime, is the FBI's Law Enforcement Online (LEO). However, many law enforcement officers need access to broader information than is contained in LEO, including private-sector specialists and technical data. A multilevel secure network could address this need.

Management and awareness support. Senior law enforcement managers and elected officials need to become better educated about the growth and impact of electronic crime on their communities and the need to establish and support dedicated computer crime units.

Many participants expressed concern that senior managers do not fully understand the impact of electronic crime and the level of expertise and tools needed to investigate and prepare cases for successful prosecution. It is often the case that managers do not realize the impact of Internet and electronic crime in their jurisdiction or in society in general.

Senior management often lacks statistical data on electronic crime, has insufficient funding and personnel resources to create electronic crime units and, in some cases, is unconvinced that electronic crime deserves much attention.

The police chiefs and managers who are willing to support an investigative capability for electronic crime often must do so at the expense of other units, or they assign dual investigation responsibilities to personnel.

Investigative and forensic tools. There is a significant and immediate need for up-to-date technological tools and equipment for State and local law enforcement agencies to conduct electronic crime investigations.

Most electronic crime cases cannot be properly investigated and developed without essential cybertools, software, and exposure to higher end computer technology.

Computer systems, software, hardware, intrusion detection tools, decryption technology, and other forensic equipment are expensive and beyond the budgets of most local law enforcement agencies. Even when special equipment is available, it is frequently out of date or incapable of being used for forensic investigations. Insufficient data storage capacity—to properly copy and analyze evidence—is a common problem, too.

Structuring a computer crime unit. As law enforcement agencies begin to address electronic crime, they grapple with how best to structure a computer or electronic crime unit that will adequately investigate crimes involving computers and properly seize and thoroughly analyze electronic evidence.

Where does the electronic crime unit belong in the law enforcement agency? Who should be a part of the unit? How should the duties of investigation and the duties of forensic analysis be separated, if at all? The experts are divided over these questions, especially the issue of whether it is better to maintain computer forensics labs with specially trained investigators or with civilian systems technicians.

DOJ would provide a very valuable service to State and local law enforcement agencies if it undertook research to capture the best thinking on the issues confronted when police agencies begin to establish better electronic crime investigation capabilities.

The experience of successful existing units should be thoroughly documented along with measures of impact related to different staffing configurations. Results of such research should be widely distributed and used as part of direct technical assistance to State and local agencies.

Conclusion

State and local law enforcement entities will face ever-increasing challenges in investigating and prosecuting Internet and other high-tech crimes. The Internet and high-tech telecommunications have created an environment in which interpersonal and commercial relationships will increasingly involve interstate and international transactions, while State and local authorities remain bound by much narrower jurisdictional limitations.

Critical infrastructure protection is an issue with which Federal, State, and local law enforcement will have to contend in the future. Increasingly, critical national functions depend on information networks and are thus susceptible to disruption or security breaches by unauthorized persons. Moreover, it is now possible to attack these infrastructures with far less preparation and expense than in the past. State and local law enforcement agencies are frequently the recipient of threats against critical infrastructure components and, many times, are the first responders to attacks on them.

Addressing these issues and the Critical Ten that emerged from this research must become a high priority. An analysis comparing the key priorities of State and local law enforcement to existing Federal training and technology programs should be the next logical step. Both this action and future study are essential if law enforcement is to realistically combat this crime.

Notes

1. U.S. Department of Justice, "Operation Derailed," United States Attorney's Office, Northern District of Georgia, Atlanta, GA, 1999.

2. D.J. Icove, "Collaring the Cybercrook: An Investigator's View," *Spectrum* (June 1997).

3. W.P. Williams, T.A. Bresnick, and D.M. Buede, "Summary Report of Focus Groups," National Cybercrime Training Partnership, U.S. Department of Justice, Criminal Division, Computer Crime and Intellectual Property Section, Washington, DC, January 1998; W.P. Williams, "The National Cybercrime Training Partnership," *The Police Chief* (February 1999).

4. D.J. Icove, V.B. Wherry, and J.D. Schroeder, *Combating Arson-for-Profit: Advanced Techniques for Investigators*, Columbus, OH: Battelle Press, 1998.

5. Michael A. Vatis, comments regarding "Issues and Trends: 1999 CSI/FBI Computer Crime and Security Survey," San Francisco, CA, 1999.

This project synopsis is derived from a full report sponsored by NIJ and undertaken by a multiorganization project management team. The team included NIJ Project Directors Saralyn Borrowman and Amon Young; Hollis Stambaugh and David Beaupre, TriData Corporation; Dr. David J. Icove, U.S. Tennessee Valley Authority Police; Richard Baker and Wayne Cassaday, U.S. Navy Space and Naval Warfare Systems Command; and Wayne P. Williams, U.S. Department of Justice, Criminal Division, Computer Crime and Intellectual Property Section.

The study reported in this Research in Brief was cofunded through an interagency agreement with the Tennessee Valley Authority and the National Institute of Justice, U.S. Department of Justice, under grant number 98–DT–R–076.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance, the Bureau of Justice Statistics, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime.

Findings and conclusions of the research reported here are those of the authors and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

This and other NIJ publications can be found at and downloaded from the NIJ Web site (http://www.ojp.usdoj.gov/nij).

NCJ 183451

U.S. Department of Justice
Office of Justice Programs
National Institute of Justice

Washington, DC 20531

Official Business
Penalty for Private Use $300

PRESORTED STANDARD
POSTAGE & FEES PAID
DOJ/NIJ
PERMIT NO. G–91