



0047-2352(94)00042-5

THE FUTURE OF HIGH-TECHNOLOGY CRIME: A PARALLEL DELPHI STUDY

LARRY E. COUTORIE

Office of the Director of Police
The University of Texas System
Austin, Texas 78701

ABSTRACT

This study attempts to forecast the future nature of high-technology crime. High technology can be defined as a form of sophisticated electronic device—computer, cellular telephone, and other digital communication—that is in common use today. Criminal activity involving these devices now usually takes the form of manipulating the device to aid in the performance of some criminal activity, such as using cellular telephones in drug deals to thwart government intervention or a computer program to achieve a theft of money or data. Technology changes at an astounding rate while law enforcement techniques, which traditionally are reactionary, do not.

INTRODUCTION

This study attempts to forecast the future nature of high-technology crime. Due to the broad spectrum of high technology available, a Delphi inquiry was chosen to gather information. The groups of experts include nine from traditional law enforcement backgrounds and a parallel group of seven highly proficient “hackers,” some of whom have engaged in illegal activities in the past.

It is important that the term *hacker* be defined for the purpose of this study. The term originates from an adept group of student computer programmers attending the Massachusetts Institute of Technology in the late

1950s. At that time, even large mainframe computers had very limited memory and, therefore, programs had to be very small and efficient. As a programmer, the measure of one’s expertise was to write a program in as few lines as possible. As the program routines were improved, one was said to have “hacked” a few lines from it.

This group also participated in a large model railroad setup as a hobby. Any one of the group was welcome to change the railroad setup as long as he improved its operation. This ethic carried over to programming, and they felt free to improve each other’s programs by “hacking” lines of code as long as this change did not alter the nature of the

program. This eventually led to looking into the programs of others outside the group and attempting to improve them. No harm to the computers or programs of others was intended. Those who did damage computers or programs have become known as "crackers" and generally are not held in high regard by "hackers."

A REVIEW OF THE LITERATURE

The Future of High-Technology Crime

A survey of some recent predictions made by experts produced the following: According to Gregson (1986), armed robbers will virtually disappear by 2001 because of a cashless society and the prevalence of electronic fund transfers. Counterfeiting is predicted to increase through the use of high-technology paper copiers and "instant photocopying." Gregson sees a change in the types of theft from cash and negotiable instruments to "physical possessions." Thieves will now "barter" these physical possessions to sophisticated computer criminals who will pay for them with electronic cash transfers to the thief's checking account. Property protected with implanted microprocessors to prove and trace ownership will be vulnerable because of electronic unscramblers and security neutralizers. Even as computers and electronics become more secure, future computer pirates will find methods of entry into "protected" areas.

The immediacy of the rise in high-technology crime is illustrated by a Delphi study conducted by FBI Agent William L. Tafoya (1986). He predicted a more than 50 percent increase over the 1984 level in computer-related crimes by 1990 and that high-technology crimes by the year 2000 will be so complex that police will only be able to take preliminary reports.

Jay S. Albanese (1988) predicts thieves also will be more sophisticated in the future. He cites an example of improvements to bank safe technology and more sophisticated methods to defeat typical security measures. In another example, Albanese describes innovations used by criminals to circumvent fraud prevention

TABLE 1
AGES OF OFFENDERS ARRESTED FOR
FRAUD-RELATED CRIMES

	Median Age, 1965-1985			
	1970	1975	1980	1985
United States	27.9	28.9	30.0	31.5
Canada	26.5	28.0	29.9	31.9

(Albanese, 1988:28)

with credit cards—from using stolen cards, countered by electronic "real-time" reporting by the banks computer, to the scavenging of carbons from trash bins for legitimate numbers with which to create electronically forged cards not yet reported as stolen by their owners. Albanese notes:

Rapid changes in technology generate opportunities for theft that can be exploited by criminals for financial gain. Only after thieves experience some success does the government, or private industry, take steps to reduce the opportunities for theft. This improvement in detection and/or prevention technology must then be matched, or surpassed, by criminals if they are to avoid apprehension. (Albanese, 1988:25)

Albanese observes that theft has traditionally been a crime of stealth, requiring speed and agility. The aging of the North American population has forced criminals to use fraud as a means of theft since they now lack this speed and agility and are more educated than their predecessors (see Tables 1 and 2).

Santa Clara, California, County Deputy District Attorney Kenneth Rosenblatt cites specific incidents of computer crimes:

Our society is about to feel the impact of the first generation of children who have grown up using computers. The increasing sophistication of hackers suggests that computer crime will soar as members of this new generation are tempted to commit more serious offenses. Besides raising prices, computer crime endangers our country's telecommunications systems, since phone-company switching computers are

vulnerable to sabotage. The spread of scientific knowledge is also at risk; to prevent "viral" infections, research institutions may have to tighten access to their computer networks. (Rosenblatt, 1990:1)

Current High-Technology Crime

The accuracy of these predictions may be indicated by the following excerpts from recent articles in *USA Today*.

A new breed of high-technology criminal has found a way to use your credit card—even if you never have. Last week, San Diego police announced an investigation into a ring of computer hackers who have broken into several financial data bases, including the files of Equifax, one of the nations largest credit-reporting agencies. (*USA Today*, 27 April 1992:6B)

Two Cornell University students have been accused of creating a computer virus, called MBDF-A, that infected computers around the world. David Blumenthal, 20, and Mark Pilgrim, 19, face a maximum four years in prison for allegedly hiding the virus in three Macintosh computer games that were sent via phone link from Cornell's computer center to an archive at Stanford University. Macintosh PC's across the USA, Great Britain and Japan were infected when users obtained the game through phone lines. Once in the Macs, the virus wiped out the operating software. (*USA Today*, 21 May 1992:7B)

Filing your tax return by computer has grown in popularity since the Internal Revenue Service introduced the program in 1986. Today, one of the fastest growing tax scams involves electronic filing. Real names and social security numbers were used to file false tax returns indicating a refund was due. Loans were made against the refunds when the IRS confirmed receipt of the returns. The total loss was \$1 million. The perpetrator was sentenced to 15 years and \$300,000 in fines. (*USA Today*, 15 June 1992:3B)

Federal officials have charged a California man with a computer crime that reads like a Tom Clancy suspense novel. Disgruntled, underappreciated worker plants a "logic bomb" program to destroy data in the computer system

of a defense electronics company, then quits. He sets the bomb to go off months later, hoping he will be brought back as the hero to fix the damage. But a co-worker stumbles onto the bomb and it is defused before any damage is done. (*USA Today*, 27 June 1992:1B)

All sorts of revenue are susceptible to high-technology manipulation. A report in *Billboard* (Borzillo, 1993) details the seizing of incoming phone lines by computer to manipulate the winning caller of radio contests of three Los Angeles radio stations, the perpetrator was a twenty-seven-year-old computer cracker. Richard Behar (1993) reported on the arrest of Stew Leonard, the owner of two popular food stores in Connecticut, who plead guilty to using a computer program to reduce profits on the sales figures allowing him to skim \$17 million in cash. Robert A. Mamis (1993) details how an estimated \$4 billion in uncollectible phone bills were run up by phone phreaks, computer crackers specializing in breaking into telephone company computers or otherwise illegally obtaining and using phone credit card numbers to make long distance calls. Both large companies like Mitsubishi International (\$430,000) and small businesses like Love's Country Stores (\$7,500) are susceptible to this form of fraud which happens every day.

Lamont Wood (1993) details how desktop publishing has advanced to the point of being a relatively easy vehicle to use to forge a number of different documents. Letters of reference with signatures, government checks, drivers' licenses, and phony invoices are just a few examples of the way this high-technology software and hardware are being abused. In

TABLE 2
NUMBER OF FRAUD-RELATED CRIMES

	Fraud Rates (per 1,000)		
	1965	1985	% of Change
United States	38.8	141.3	+264
Canada	197.5	486.0	+146

(Albanese, 1988:28)

Connecticut, Kelley Holland and Paul Eng (1993) report on high-technology bandits who installed a fake automatic teller machine (ATM) in a shopping mall to capture electronic account numbers and personal identification numbers (PINs) that eventually allowed them to steal \$50,000. Holland and Eng state that ATM use now accounts for over \$7.2 billion worth of transactions annually. This fact may make them an attractive target in the future.

The greatest repositories of information in the world, universities, are prime targets for computer crackers. They are relatively open and easy to access through the internet. Additionally, software security holes are increasingly more widely known before they can be patched. David L. Wilson (1994) reports of a recent raid by crackers into the computers of Rice University where administrators were forced to shut down the university's links with the internet for a week to regain control of the computer accounts of students and faculty members that had been taken over by the crackers. This denied the use of the internet to Rice users for a week. Rice was not the only university mentioned in the report and many, when contacted, denied being attacked. It is a regular occurrence, however, at different levels of severity at universities throughout the world via the internet.

The innovativeness allowed by the technology and used by the criminals is great and widely varied. The need to predict the nature and direction of high-technology crime has been widely recognized. Given the speed of change of high technology, the need for rapid and accurate predictions is even more vital. Law enforcement could fall far enough behind the curve to be left behind forever in the quest to control high-technology crime. Proactive planning is one important tool to keep this from happening.

Some agencies are keeping up with the technology as well as they can, expectedly, the agency is in one of the high technology centers of the country. Los Angeles County Sheriff's Department makes use of computerized data bases to search for leads on bits of information that would otherwise be much too little to justify the time of an investigator.

Jonathan Walters (1990) reports their use of the department's computerized reporting system to search for a vehicle based only on color and make to help solve a drive-by shooting. If the information had been handled traditionally it would have been written down on a three-by-five card, filed, and effectively lost.

METHODOLOGY

The Future of High-Technology Crime

The preceding information seems to beg the question: What do we have to look forward to in the arena of high-technology crimes and what do we do about it? The objective of this study, therefore, was to forecast the direction and form that high-technology crime might take over the course of the next ten years. To accomplish this goal, a Delphi study was devised using the opinions of recognized and "nontraditional" experts.

Experts were selected from recommendations by peers in the field of law enforcement dealing specifically with high-technology crime. Selection considerations included their experience in areas such as high-technology law enforcement training, computer-related law enforcement field experience, government computer-related management, and a very knowledgeable civilian perspective, all on a national scope. The "nontraditional" experts were recommended by experts in the field of computer science and, where possible, these recommendations were verified independently through newspaper records and background checks. To analyze the results, the Delphi technique, a recognized methodology of forecasting the probability of future events, was chosen for this study.

The Delphi Technique

The Delphi technique was first developed by Olaf Helmer and Norman Dalkey at the Rand Corporation in the early 1950s to obtain a consensus opinion from a group of experts. This technique has participants complete several related questionnaires. The participants

in this study remained anonymous to each other during the process so the input/output was neither skewed by personalities nor other factors relevant in face-to-face situations. The two groups of experts were handled separately to discover if there were any similarities and differences in their opinions.

Initially, both sets of participants were asked to answer the same five questions. In this first round, the questions were intentionally left "open ended" to allow the participants to have free reign in formulating their answers. Their answers were then used to create questions on the second questionnaire. Responses were analyzed to determine the consensus of the group using the semi-inter-quartile range of the data from each item. Each group was then asked to agree/disagree with information on a questionnaire. Time constraints limited the number of participants and allowed for only three questionnaires.

The Participants

The following is a list of the "traditional" experts along with a brief biographical sketch:

1. James Christy II—director of Computer Crime Investigations, Investigative Operations Center, Air Force Office of Special Investigations, Bolling Air Force Base, Washington, D.C.; case agent in the Hanover Hacker case related in "The Cookoo's Egg" (Stoll, 1989).
2. William Cook—former assistant United States attorney in Chicago, Illinois; now in private practice.
3. Fred Cotton—training manager for the Search Group.
4. Carlton Fitzpatrick—computer crime fraud and investigation instructor at the Federal Law Enforcement Training Center.
5. J. Michael Gibbons—supervisory special agent, Federal Bureau of Investigations; computer crime specialist.
6. Richard P. Kusserow—tracked fraud, waste, and abuse in computers in a number of government organizations; now senior vice-president of Strategic Management Associates; former inspector general, Department of Health and Human Resources; former

agent, Federal Bureau of Investigations; recipient of a 1988 presidential citation.

7. John Markoff—computer crime reporter for the *New York Times* and author of *Hacker*.
8. William Tafoya, Ph.D.—special agent, Federal Bureau of Investigations; futurist.
9. Robert W. Taylor, Ph.D.—former police officer; currently an associate professor of public administration and criminal justice at The University of Texas at Tyler, Texas.

The "nontraditional experts," and their computer aliases, are:

1. Bruce Fancher, dead lord—former Legion of Doom member; former contributor to "2600"; network hacker.
2. Stu Klingman, shiva—legitimate programmer with published articles who is very knowledgeable about network hacking.
3. Pat Kroupa, lord digital—former Legion of Doom member; now contributing author to "Mondo 2000"; computer business owner.
4. Craig Neidorf, knight lightning—law student; former telephone system phreaker.
5. Lynn Rose, terminus—former "cracker" who was federally convicted of involvement in pirating UNIX source code.
6. Craig Stockwell, chromsync—former "cracker" now earning his degree while working as a computer system operator; plans a career in law enforcement or computer technology.
7. FNU LNU, lex luthor—a founding member of the Legion of Doom; has earned a master's degree in engineering; currently a partner in a computer-related business; has published an article on computer security under his real name.

First Questionnaire

The first round of questions was formulated from some general areas of concern regarding high-technology crime.

1. In your opinion, what area(s) of high technology will be the focus of criminal activity in the next ten years?
2. What form(s) do you believe this activity will take?
3. What steps should be taken now to prepare the police to combat this criminal activity?
4. Do you believe the responsibility for criminal investigation of high-technology crimes

will be primarily that of government or private businesses? Why?

5. Do you believe the responsibility for crime prevention activities regarding high-technology crimes will be primarily that of government or private businesses? Why?

The same first-round questions were submitted to both groups beginning mid-October, 1992. The study began to diverge because the viewpoints of the groups were very different. The first-round answers of each group were studied for main points and ideas, and these were compiled and formulated into the second round of questions.

The Second Questionnaire

In the second questionnaire, each first-round question was restated and expanded upon with more specific information gleaned from the answers to the first questionnaire from the individual groups. Participants in the two groups were asked to respond to these times by indicating how strongly they agreed or disagreed with these specific questions. Additional comments were encouraged. A numerical rating was created in order to perform a statistical analysis of the responses. The respondents were asked to rate the degree to which they agreed or disagreed with each statement according to the following scale:

- 1 = Strongly agree
- 2 = Agree
- 3 = Moderately agree
- 4 = Uncertain
- 5 = Moderately disagree
- 6 = Disagree
- 7 = Strongly disagree

The Questionnaire for the Traditional Experts

The following list of questions and answers was derived from the answers by the traditional experts to the first round of questions:

1. In your opinion, what area(s) of high technology will be the focus of criminal activity in the next ten years?
 - a. Electronic terrorism and sabotage.
 - b. Child pornography.
 - c. Compromise of cryptology systems.
 - d. Cellular communications.
 - e. Automated teller transactions.
 - f. Attacks on radio/satellite communications.
 - g. Electronic counterfeiting.
 - h. Communications interception for profit.
 - i. Use of high technology for secure communications by criminal groups.
 - j. Industrial espionage.
 - k. Counterfeit computer hardware components.
 - l. Information/data theft.
 - m. Theft of biomedical research.
 - n. Communications technology.
 - o. Information/data manipulation.
 - p. Vulnerability of individuals.
 - q. More sophisticated fraud schemes.
 - r. Vulnerability of computer networks.
2. What form(s) do you believe this activity will take?
 - a. Increased incidents of financial fraud.
 - b. Voter fraud made possible by the use of wide area networks for voting.
 - c. Attacks on computer systems by fanatic domestic groups.
 - d. The increased vulnerability of individual's information due to increased use of wide area networks.
 - e. Decreased incidents of telecommunications crime due to advances in technology preventing them.
 - f. The terrorist's use of highly technological destructive devices like magnetic pulse generators.
 - g. Increased sophistication of criminals in their use of high technology.
 - h. Increased thefts from automobiles of portable computer equipment (i.e., laptop computers).
 - i. Increased sophistication of pornography due to virtual reality capabilities.
 - j. New legal questions regarding computer generated child pornography (since no actual human victim may be involved).
 - k. The increased entry into counterfeiting by amateurs because of the availability of easy-to-use high technological tools.
 - l. An increase in the level of digitized child pornography transmitted by computer, especially since enforcement of laws regarding its transmission by mail has increased.

- m. Increased incidents of electronic counterfeiting.
 - n. The use of encryption by criminals to subvert law enforcement.
 - o. Increased use of electronic bulletin boards for secure communications by criminals.
 - p. Increases in industrial espionage by third-world countries to compete in an increasingly high-technology global marketplace.
 - q. Attacks on computer systems to hide or destroy evidence of high-technology crimes.
 - r. Increased pirating of computer software.
 - s. Increased malicious attacks on computer systems.
 - t. Perpetration of such crimes as murder by hacking into medical records and intentionally changing medications/dosages.
 - u. Alteration of software or software written specifically for a criminal purpose.
 - v. Increased domestic industrial espionage.
 - w. Information/data theft.
 - x. Information/data held hostage.
 - y. Terrorist attacks on computer systems.
3. What steps should be taken now to prepare the police to combat this criminal activity?
- a. The introduction of computers as an investigatory tool.
 - b. Police need to change their perspective regarding who criminals are and what they do.
 - c. Change recruiting tactics to seek personnel with talent/experience in high-technology matters.
 - d. Mandated training for all officers to begin even at a basic academy level.
 - e. Encouragement of more cooperation between private business and police in investigations.
 - f. Restructuring of legislation to be more appropriate to high-technology crimes, traditional elements of crime are not always appropriate.
 - g. Further education of law enforcement management as to the magnitude of the problem.
 - h. Organization of task forces or response teams at a state/local level made up of members with individual areas of expertise.
 - i. Rethinking traditional jurisdictional concepts to allow more cooperation between agencies.
 - j. Establishment of high-technology forensic laboratories to assist in investigations.
- k. Establishment of dedicated high-technology criminal investigation units at federal levels.
 - l. Establishment of dedicated high-technology criminal investigation units at *all* levels.
4. Do you believe the responsibility for criminal investigation of high-technology crimes will be primarily that of government or private businesses? Why?
- a. Government, due to the sensitivity of some investigations, must remain responsible for investigations.
 - b. The responsibility will always be a primary duty of government because of contradictory goals in investigations.
 - c. Private businesses will continue to take responsibility until the problem becomes catastrophic.
 - d. Private businesses, because of the reluctance of government to become involved with high-technology crimes.
 - e. Government, because of a legal and ethical mandate to protect the rights of individuals.
 - f. Private businesses, even as contractors to government agencies.
5. Do you believe the responsibility for crime prevention activities regarding high-technology crimes will be primarily that of government or private businesses? Why?
- a. The primary responsibility rests with the government which is charged with providing this service to our citizens.
 - b. Education will be the responsibility of government, but the actual security will be the responsibility of private businesses.
 - c. Both, however, private industry is doing a much better job at warning and training themselves.
 - d. Private businesses, in the sense that new security technologies more readily come from the private sector.
 - e. Private businesses; government will never have the resources to have an impact in this area.

*The Questionnaire for the
Nontraditional Experts*

The following list of items was derived from the first-round answers by the nontraditional experts:

1. In your opinion, what area(s) of high technology will be the focus of criminal activity in the next ten years?
 - a. Attacks on computer systems/networks via telecommunications.
 - b. Industrial espionage.
 - c. Financial fraud by use of computers/high technology.
 - d. Counterfeiting by use of computers/high technology.
 - e. Forgery by use of computers/high technology.
 - f. Attacks on information systems by telecommunication.
 - g. Data manipulation/theft by use of computers/high-technology.
 - h. Biotechnological engineering abuses.
2. What form(s) do you believe this activity will take?
 - a. Attacks on data bases to control information.
 - b. Attacks on miniserver workstations.
 - c. Violations of privacy of individuals due to data base invasions.
 - d. A continuation of software piracy.
 - e. Increased occurrences of data base invasions and data theft.
 - f. Increased occurrences of industrial espionage.
 - g. Increased occurrences of counterfeiting perpetrated by computer.
 - h. Increased occurrences of fraud involving credit cards by telecommunications because of better in-store verifications.
 - i. Increased occurrences of credit card fraud perpetrated by computer.
 - j. Use of encryption by criminals to subvert police investigations.
 - k. Increased occurrences of use of software written specifically for criminal purposes.
 1. Increased attacks on computer systems allowed by faster and more advanced hardware technology.
 - m. Increased occurrences of counterfeiting perpetrated by computer.
 - n. Increased occurrences of financial fraud perpetrated by computer.
 - o. Alteration of government data stored for purposes of evidence.
 - p. Manipulation of digitized images to alter apparent factual situations.
 - q. Biological terrorism.
 - r. Biotechnological engineering of new drugs.
 - s. Vulnerabilities of networks allowed by new software not properly protected.
3. What steps should be taken now to prepare the police to combat this criminal activity?
 - a. Special schools should be established for high-technology investigations training.
 - b. Law enforcement should take a team approach to investigations, pairing an officer with a computer technician.
 - c. Protected audit trails that do not allow alterations to aid investigations.
 - d. User security should require more and/or better authentication systems.
 - e. Law enforcement should take a more proactive approach on crime prevention.
 - f. More education for law enforcement officers on computer operations and vulnerabilities.
 - g. A change in recruitment of new officers, selecting those able to work in, or with an interest in, high-technology areas.
 - h. Infiltration of organizations for purposes of gathering intelligence.
 - i. The establishment of new laws regarding data integrity to protect citizens from the consequences of illegally altered data.
 - j. The development of new means to protect the authenticity of data.
4. Do you believe the responsibility for criminal investigation of high-technology crimes will be primarily that of government or private businesses? Why?
 - a. Government because they have more resources available to investigate these types of crimes.
 - b. Government because businesses cannot afford to hire the investigators with the necessary level of expertise to investigate these types of crimes.
 - c. This will require a combined effort of specially trained investigators and will not be able to be accomplished with a "cookbook" approach by existing investigators.
 - d. Private businesses will have to investigate these crimes except for government intervention when the investigation gets to the point of arrest.
5. Do you believe the responsibility for crime prevention activities regarding high-technology crimes will be primarily that of government or private businesses? Why?
 - a. Private businesses because government is not in a position to prevent these types of crimes as well as investigate them.

- b. Private businesses, but allow tax credit to offset the expense of the crime-prevention activities.
- c. Both, however, private businesses are primarily responsible for crime prevention.
- d. In some high-technology areas (such as biotechnology), the government will have to help by controlling equipment and/or materials needed to commit crimes.

The Third Questionnaire

The second-round responses were statistically analyzed to determine an inter-quartile score for each item and were grouped into the areas of consensus. Revised questions and answers, indicating levels of consensus on each item, were resubmitted to each group as the third and last questionnaire, along with a request for final comments.

Responses from the Traditional Experts

Tables 3 through 6 are based upon responses from the third round submitted to the traditional expert group. The letter in parentheses corresponds with the item on the questionnaire. Child pornography, property crimes, data manipulation, and the criminal use of cryptology are some key areas of importance identified by this group. Conversely, the areas of electronic terrorism and code breaking received lower priorities as areas of concern.

Responses from the Nontraditional Experts

Tables 7 through 11 are based upon responses from the third round submitted to the nontraditional group. The letter in parentheses corresponds with the item on the questionnaire. This group seems more concerned with actual intrusions via telecommunications into computers for purposes of data manipulation and fraud. Some confusion exists, however, in that attacks on information systems via telecommunications were also identified as an area of low consensus.

SUMMARY

First-round responses from the two groups expectantly differed. This led to different second-round topics for each individual group. As a result, subsequent polling of the two groups diverged somewhat. Because of these differences in first-round responses, no statistical comparison was made regarding Table 12, which combines their responses; however, both groups ultimately appeared to share a consensus in five areas.

Both groups agree that the focus of new criminal activity will include attacks on computer systems and the use of computers to commit fraud and manipulate data. These activities are likely to come in the form of counterfeiting, financial fraud, and software piracy. Advancements in computer technology itself will assist in the commission of these types of crime. The groups mutually agree that the burden to initially investigate high-technology crime will, at least for the time being, fall on private businesses with their greater resources. Private businesses also will need to work jointly with the government on follow-up investigations. Private businesses are also responsible for protecting their own assets, but government should aid in making them aware of the threats to those assets. It was surprising to see that there was no mention of computer viruses in the responses from both groups, but these are considered to be a minor threat and easily defended against, at least for the time being.

CONCLUSIONS

The literature review has predicted the continued rise in high-technology crime, and current literature appears to support this prediction. There are certainly many reports of occurrences from a number of different sources. The responses to the questionnaires shed some light on the future of this area of law enforcement.

The consensus of the traditional experts seems to predict more of an emphasis on the

TABLE 3

AREAS OF HIGH CONSENSUS: TRADITIONAL EXPERTS (INTER-QUARTILE RANGE OF ≤ 1.5)

<i>High-Tech Crime Areas</i>	<i>Form of Activity</i>	<i>Preventive Steps</i>	<i>Investigative Responsibility</i>	<i>Prevention Responsibility</i>
Child pornography (b)	Increased incidents of financial fraud (a)	Change definitions of criminals and criminal activity (b)	Government due to sensitivity of some investigations (a)	Government because it's charged with providing this service (a)
Radio/satellite attacks (f)	Voter fraud via wide area networks (b)	Change recruiting methods to seek personnel with high-tech training and/or knowledge (c)	Government because of contradictory goals in investigations (b)	Government will provide education while private businesses provide actual security (b)
Electronic counterfeiting (g)	Increasingly sophisticated criminals using high technology (g)	Train all law enforcement officers (d)	Private businesses until problem becomes catastrophic (c)	Private businesses because new security technologies come from private sector (d)
Communications interception for profit (h)	Theft of portable computers from automobiles (h)	More cooperation between private business and police in investigations (e)	Private businesses because of government's reluctance to be involved in high-tech crimes (d)	
Criminal groups using high technology to secure communications (i)	More sophisticated pornography using virtual reality capabilities (i)	Restructure legislation for high-tech crimes (f)	Government because of legal and ethical mandates to protect individual rights (e)	
Industrial espionage (j)	New legal questions about computer-generated child pornography (no human victim) (j)	Educate law enforcement managers about magnitude of high-tech crime (g)	Private businesses as contracts to government agencies (f)	
Counterfeiting computer hardware components (k)	Increased counterfeiting by amateurs via high-tech tools (k)	Create task forces or response teams with appropriate expertise (h)		
Theft of information/data (l)	Increased transmission of digitized child pornography (l)	Rethink jurisdictions to allow more inter-agency cooperation (i)		
Communications technology (n)	Increased incidents of electronic counterfeiting (m)	Create high-tech forensic labs that assist in investigations (j)		
Manipulation of information/data (o)	Criminals using encryption to subvert law enforcement (n)	Create federal high-tech criminal investigation units (k)		
Individual's vulnerability (p)	Increased use of electronic bulletin boards (o)	Create high-tech criminal investigation units at all levels (l)		
More sophisticated fraud schemes (q)	Sabotaging computer systems to destroy evidence (q)			
Computer network vulnerabilities (r)	Increased pirating of computer software (r)			
	Malicious sabotage of computer systems (s)			
	Tailoring and designing software for criminal purposes (u)			
	More domestic industrial espionage (v)			
	Theft of data and/or information (w)			
	Holding data and/or information hostage (x)			

TABLE 4
AREAS OF MODERATE CONSENSUS: TRADITIONAL EXPERTS
(INTER-QUARTILE RANGE OF ≥ 1.5 – ≤ 2.5)

<i>High-Tech Crime Areas</i>	<i>Form of Activity</i>	<i>Preventive Steps</i>	<i>Investigative Responsibility</i>	<i>Prevention Responsibility</i>
Cellular communications (d)	Greater vulnerability of individual information from more use of wide-area networks (d)	Introduce computers as an investigatory tool (a)		Private businesses because government lacks adequate resources to make an impact 'e)
Automated teller transactions (e)	Increased incidents of electronic counterfeiting (m)			
Theft of biomedical research (m)	Increased industrial espionage by third-world countries to compete in high-tech global marketplace (p) More crimes from tampering with medical records/altering medications and dosages (t) Terrorist attacks on computer systems (y)			

TABLE 5

AREAS OF LOW CONSENSUS: TRADITIONAL EXPERTS (INTER-QUARTILE RANGE OF ≥ 2.5 – ≤ 3.5)

<i>High-Tech Crime Areas</i>	<i>Form of Activity</i>	<i>Preventive Steps</i>	<i>Investigative Responsibility</i>	<i>Prevention Responsibility</i>
Electronic terrorism and sabotage (a)	Attacks on computer systems by fanatic domestic groups seeking revenge (c)			Both, but private industry is doing a better job at warning and training themselves (c)
Compromising cryptology systems (c)	Fewer incidents of telecommunication crime from advances in preventive technology (e)			

TABLE 6

AREA OF QUESTIONABLE CONSENSUS: TRADITIONAL EXPERTS
(INTER-QUARTILE RANGE OF ≥ 3.5 – ≤ 4.5)

<i>High-Tech Crime Areas</i>	<i>Form of Activity</i>	<i>Preventive Steps</i>	<i>Investigative Responsibility</i>	<i>Prevention Responsibility</i>
	Terrorists' use of technologically destructive devices such as magnetic pulse generators (f)			

TABLE 7

AREAS OF HIGH CONSENSUS: NONTRADITIONAL EXPERTS (INTER-QUARTILE RANGE OF ≤ 1.5)

<i>High-Tech Crime Areas</i>	<i>Form of Activity</i>	<i>Preventive Steps</i>	<i>Investigative Responsibility</i>	<i>Prevention Responsibility</i>
Attacks on computer systems and networks via telecommunications (a)	Attacks on data bases to control information (a)	Establish special schools for high-tech investigation training (a)	Government because it has more resources to investigate new types of crimes (a)	Both, but private businesses are primarily responsible for crime prevention (c)
Financial fraud using computers and advanced technology (c)	Attacks on miniserver workstations (b)	Team approach: Pair officer with computer technician (b)	Combined effort of specially trained investigators, no "cook-book" approach with existing investigators is workable (c)	
Data manipulation and theft by using computers or advanced technology (g)	Continued software piracy (d)	User security should improve authentication systems (d)	Private businesses will have to investigate; government intervention at time of arrest (d)	
Biotechnological engineering abuses (h)	Increased occurrences of industrial espionage (f)	Increase education for law enforcement officers in computer operations and vulnerability (f)		
	Increased occurrences in counterfeiting using a computer (g)	Recruit new law enforcement officers having ability or interest in high-tech areas (g)		
	Increased occurrences of fraud involving credit cards via telecommunication due to improved in-store verifications (h)	Write new laws concerning data integrity as protection from illegally altered data (i)		

TABLE 8
AREAS OF MODERATE CONSENSUS: NONTRADITIONAL EXPERTS
(INTER-QUARTILE RANGE OF ≥ 1.5 - ≤ 2.5)

<i>High-Tech Crime Areas</i>	<i>Form of Activity</i>	<i>Preventive Steps</i>	<i>Investigative Responsibility</i>	<i>Prevention Responsibility</i>
Industrial espionage (b)	Violations of privacy from data base invasions (c)	Law enforcement should take more proactive approach on crime prevention (e)	Government because businesses cannot afford investigators with adequate expertise (b)	Government has the responsibility for education, but actual security is responsibility of private businesses (b)
Counterfeiting using computer or advanced technology (d)	Increased occurrences of data base invasions and data theft (e)			
Forgery by using computer or advanced technology (e)	Increased attacks on computer systems by using advanced hardware technology (l) Increased occurrences of counterfeiting using a computer (m)			

TABLE 9

AREAS OF LOW CONSENSUS: NONTRADITIONAL EXPERTS (INTER-QUARTILE RANGE OF ≥ 2.5 - ≤ 3.5)

<i>High-Tech Crime Areas</i>	<i>Form of Activity</i>	<i>Preventive Steps</i>	<i>Investigative Responsibility</i>	<i>Prevention Responsibility</i>
Attacks on information systems via telecommunication (f)	Criminals using encryption to subvert police investigations (j) Biotechnological engineering of new drugs (r)	Create protected audit trails that do not allow alterations (c)	Government must help in some high-tech areas (biotechnology) by controlling equipment or materials needed to commit crime (d)	

TABLE 10

AREAS OF QUESTIONABLE CONSENSUS: NONTRADITIONAL EXPERTS
(INTER-QUARTILE RANGE OF ≥ 3.5 - ≤ 4.5)

<i>High-Tech Crime Areas</i>	<i>Form of Activity</i>	<i>Preventive Steps</i>	<i>Investigative Responsibility</i>	<i>Prevention Responsibility</i>
				Private businesses because government cannot prevent and investigate these types of crimes (d)

TABLE 11

AREAS OF LOW DISSENSUS: NONTRADITIONAL EXPERTS (INTER-QUARTILE RANGE OF ≥ 4.5 – ≤ 5.5)

<i>High-Tech Crime Areas</i>	<i>Form of Activity</i>	<i>Preventive Steps</i>	<i>Investigative Responsibility</i>	<i>Prevention Responsibility</i>
		Infiltrate organizations to gather intelligence (h)		

use of computers and high technology to commit crimes as opposed to attacks on stored information, although they agreed that such attacks will probably occur. There is agreement among the traditional experts that education, training, and selective recruiting are the long-term answers. For the near future, task forces and public/private cooperation in addressing the problems may be the stop-gap measure.

The consensus of the nontraditional ex-

perts indicates that they expect computers and stored data to be more the object of crime than the traditional experts do. The nontraditional experts' opinion that high technology will be used to commit crimes parallels that of the traditional experts, however. They indicate that training and recruiting are important aspects of a department's ability to cope with future high-technology problems.

Although both groups had relatively few common areas in which they had a high con-

TABLE 12

AREAS OF CONSENSUS: TRADITIONAL AND NONTRADITIONAL EXPERTS

<i>High-Tech Crime Areas</i>	<i>Form of Activity</i>	<i>Preventive Steps</i>	<i>Investigative Responsibility</i>	<i>Prevention Responsibility</i>
Computer system attacks via telecommunications	Software piracy	Recruit individuals with computer knowledge/interest	Private businesses conduct initial investigation	Private business must protect own assets; government helps with education about potential threats
Computer-assisted fraud	Increased incidents of computer-assisted counterfeiting	Begin with teams that include civilians having needed expertise	Private business must participate in team investigations conducted by government	
Computer-assisted data manipulation or theft	Increased incidents of financial fraud	Train law enforcement officers in advanced-level computers at earlier stage of career		
	Increased attacks on computer systems via advanced technologies	Introduce new legislation and define jurisdictions to help law enforcement deal with computer crime-related matters		

sensus, there were some areas. The combined results indicate that law enforcement is heading in the right direction. High-technology crimes are going to be more sophisticated in the future, and law and law enforcement agencies appear to be ill-prepared to meet this challenge. Most have not begun to address the problem in proportion to its scope. The idea that a department can depend on its computer hobbyist to carry them through must be discarded and a specialty investigative area recognized and supported. Who would expect their department's most avid reader of Agatha Christie to be their best homicide investigator?

There is little doubt that law enforcement agencies are, at least, becoming aware of the situation. High-technology crime has not yet directly affected many individuals in society and law enforcement administrators have been reluctant to dedicate much of their limited resources to this arena of crime. If nothing is done until it becomes politically important enough to target, law enforcement will be hopelessly behind the learning and technology curves to address the problem. Enormous resources, at enormous expense, and the use of outside law enforcement will have to be brought to bear to control it.

REFERENCES

- Albanese, J. S. (1988). Tomorrow's thieves. *The Futurist* 22(5):25-28.
- Behar, R. (1993). Skimming the cream. *Time* 142(5):49.
- Borzillo, C. (1993). From contest stars to prison stripes. *Billboard* 105(19):64, 66.
- Flynn, S. (1992). Mean streets. *The Boston Phoenix*, 7-13 February, 16-18.
- Gregson, R. W. (1986). *Civilization: Its effect on the future role of the police investigation function*.
- Helmer, O. (1983). *Looking forward* (1st ed). Beverly Hills, CA: Sage Publications.
- Holland, K., and Eng, P. M. (1993). An alarm goes off at the cash machine. *Business Week*, 31 May, 39.
- McLendon, D. P. (1977). *A Delphi study of agreement and consensus among selected educator groups in Texas regarding principles underlying effective in-service education*, Unpublished doctoral dissertation, The University of Texas at Austin.
- Mamis, R. A. (1993). Fending of phone fraud. *Inc* 15(5):45.
- Rosenblatt, K. (1990). *Deterring computer crime*. Cambridge, MA: MIT Alumni Association.
- Stoll, C. (1989). The cookoo's egg: Tracking a spy through the maze of computer espionage. New York: Double Day.
- Tafoya, W. L. (1986). *A Delphi forecast of the future of law enforcement*, Unpublished doctoral dissertation, The University of Maryland.
- Walters, J. (1990). Cops and courts are turning to high-tech tools. *Governing* (October):23, 25-26.
- Wilson, D. L. (1994). Rice U. repels hacker attack. *The Chronicle of Higher Education* 40(23):A29.
- Wood, L. (1993). Don't try this at home. *Compute!* 15(8): 60-65.