HOW WILL MEDIUM SIZE LAW ENFORCEMENT AGENCIES INVESTIGATE HIGH TECHNOLOGY CRIME BY THE YEAR 2003?

TECHNICAL REPORT

BY

BRUCE K. MURAMOTO

COMMAND COLLEGE CLASS 19

COMMISSION ON PEACE OFFICER STANDARDS AND TRAINING

SACRAMENTO, CALIFORNIA

JANUARY 1995

19-0391

This Command College Independent Study Project is a FUTURES study of a particular emerging issue in law enforcement. Its purpose is NOT to predict the future, but rather to project a number of possible scenarios for strategic planning consideration.

Defining the future differs from analyzing the past because the future has not yet happened. In this project, useful alternatives have been formulated systematically so that the planner can respond to a range of possible future environments.

Managing the future means influencing the future--creating it, constraining it, adapting to it. A futures study points the way.

The views and conclusions expressed in the Command College project are those of the author and are not necessarily those of the Commission on Peace Officer Standards and Training (POST).

How Will Medium Size Law Enforcement Agencies Investigate High Technology Crime By The Year 2003?
B. K. Muramoto, Sponsoring Agency: California Commission on Peace Officer Standards and Training (POST). 1994. 148 pp.
Availability: Commission on POST, Center for Leadership Development, 1601 Alhambra Blvd., Sacramento, CA. 95816-7053
Single copies free. Order number 19-0391
National Institute of Justice / NCJRS Microfiche Program,
Box 6000, Rockville, MD. 20850
Microfiche free. Microfiche number NJC _____

Abstract

How Will Medium Size Law Enforcement Agencies Investigate High Technology Crime By The Year 2003?
Muramoto, B. K.

Consisting of two parts, a technical report and a journal style article, this study examines the impact of high technology crime investigation on medium size law enforcement agencies. The technical report focuses on ten trends and ten events that were forecast by subject matter experts during a Nominal Group Technique process. The trends identified in the study include: change in criminal law, high technology criminal investigations, organized crime, crime reporting, Cyber-Cops, hackers, computer crime victims, jurisdictional investigative boundary issues, rapid change in technology and computerized information. The panel's forecasted events include: investigation of high technology crime, high technology crime series, law enforcement partnerships, high technology terrorist attacks, entry level officer computer skills, new legislation, private funding, the use of personal communicator numbers, and high technology sales tax. A strategic and transition management plans were developed to implement a course of action. The strategic plan recommends that medium size law enforcement agencies form partnerships with public and private sector high technology crime investigation agencies. The transition plan presents the reader with a management structure and implementation plan to move the organization from its present state to the desired future state. The study's conclusions reveal that the establishment of partnerships is the best avenue for medium size law enforcement agencies to take in the investigation of high technology crime. Include in the text and appendixes are a bibliography, charts, graphs, supporting documentation and tables. The journal article focuses on the problem of high technology crime in the future and the constant evolution of new technologies.

HOW WILL MEDIUM SIZE LAW ENFORCEMENT AGENCIES INVESTIGATE HIGH TECHNOLOGY CRIME BY THE YEAR 2003?

JOURNAL ARTICLE

BY

BRUCE K. MURAMOTO

COMMAND COLLEGE CLASS 19

COMMISSION ON PEACE OFFICER STANDARDS AND TRAINING

SACRAMENTO, CALIFORNIA

JANUARY 1995

This Command College Independent Study Project is a FUTURES study of a particular emerging issue in law enforcement. Its purpose is NOT to predict the future, but rather to project a number of possible scenarios for strategic planning consideration.

Defining the future differs from analyzing the past because the future has not yet happened. In this project, useful alternatives have been formulated systematically so that the planner can respond to a range of possible future environments.

Managing the future means influencing the future--creating it, constraining it, adapting to it. A futures study points the way.

The views and conclusions expressed in the Command College project are those of the author and are not necessarily those of the Commission on Peace Officer Standards and Training (POST).

Introduction

Law Enforcement needs to open its eyes.....High-technology or computer-related crime has been around for years and is nothing new to the law enforcement community. The accounting firm of Ernest and Young estimates that high-technology crime costs US businesses about $3 to $5 billion a year in losses.[1] Search Group Inc. ,an organization of law enforcement computer-related resources, reports that other researchers would put the total loss figure as high as $40 billion per year if viruses and software piracy were included. They also report that only 6% to 11% of all computer crime is reported to law enforcement agencies. Furthermore, they indicated that only 2% of these cases result in a conviction requiring any jail time.[2]

Computer-related crime can kill.....For the most part, computer-related crime has centered around the use of computers to commit theft through electronic fund transfer fraud. In a recent article written by Deirdre Martin in Law Enforcement Technology, October, "Fighting Computer Crime", Martin reports that the San Jose Police Department recently infiltrated a computer bulletin board catering to pedophiles. They discovered a plot to kidnap a child and kill him as part as a "snuff" film. Martin reported that the conspirators were arrested in Virginia by the Federal Bureau of Investigation.[3]

Wake up and smell the coffee.....It is imperative that law enforcement managers devote more time and thought to the growing concern of high-technology crime as it relates to the future. Patricia Parker wrote an article in Police, August 1991, "Downloading Computer Crime", how police chiefs and sheriffs felt about high-technology crime.[4] In a survey conducted by the Institute of Law and Justice in Alexandria, VA, it was revealed that 75 percent of police chiefs and 63 percent of sheriffs rated computer crime investigations "as a potentially significant factor in future caseloads in their departments.[5]" However, Donn Parker states that the law enforcement community's response to high-technology crime continues to lag given the growth of the problem.[6]

Additional Problems

The private sector is experiencing a growing concern regarding who is going to investigate high-technology/computer-based crime. Current information indicates that businesses can spend up to $1 million a year trying to protect themselves against hackers and computer viruses.

Major money crimes of the past century such as bank robbery, million dollar armor car holdups, insurance fraud will seem inconsequential in the future when compared to computer-based crime. According to J. J. Bloombecker reports that computer crime costs businesses in America over $500 million a year.

According to Mark Lewny A.T. and T, M.C.I. Communications Inc., and US Sprint are among several corporations that have taken steps to monitor long-distance usage. Phone fraud losses are estimated to run from $500 million to $4 billion per year.[7]

Another survey by Kristina B. Sullivan suggests that 63 percent of the large microcomputer sites surveyed have experienced at least one computer virus attack. She believes that there is a trend towards high-technology crime happening on a global basis.[8]

According to Jane Bird, security breaches are often kept from the public to save embarrassment of the corporations. She sees a sharp increase in this type of crime over the past two years and states that the United Kingdom industry loses an average of 1.1 billion pound sterling annually through computer-related crime.[9]

August Bequai believes that few Federal and local police agencies have instituted training programs in the computer crime area. He goes so far as to say that law enforcement is ill trained and "lacks in a cohesive strategy to play an important in the war against computer crime; in addition communications between the world of business and law enforcement are at best poor."[10] Bequai adds that the private sector believes that America's present law enforcement "is a patchwork of small, often inefficient police agencies working at odds with each other." Bequai also believes that private sector management must work together with law enforcement if computer crime is to be contained.

According to Fred B. Cotton and William R. Spernow states that an "ever-increasing variety of fraud and criminal acts being perpetrated by computer." They also agree that "local law enforcement agencies are hard pressed to address this growing crime problem because most do not have investigators who have been trained to work in the high-technology environment."[11]

There are many who believe that computer crime will be the wave of the future. The children of the 1980's and 1990's have grown up with computers. They will be as adept in using computers to commit crimes as were car thieves of the 1950's using wire to "hot wire" cars.[12] Others also believe that computer crime will trend to increase in proportion to the numbers of computers in use. There is no question that, with the numbers of computers increasing high-technology crime will continue to grow in the future.[13]

The investigation of high-technology crime will be an emerging issue for law enforcement in the future. The collected data strongly demonstrates a need for law enforcement to develop strategies to properly investigate the many aspects of high-technology crime.

Issue Question

The specific issue that this Command College independent study project focuses on:

How will medium-size law enforcement agencies investigate high-technology crime by the year 2003?

The traditional mandate for law enforcement has been the investigation of criminal offenses using traditional management and expertise. In the future, computer-related crime due to its level of sophistication, may require a change in the traditional role of law enforcement because of the nature of that type of crime. The material below

illustrates only some of the problems that law enforcement will face in the future because of these developments.

Contemporary Issues

High-technology crime is a contemporary issue not only for law enforcement but for the entire nation in general. In the past year more has been written on this topic than ever before. Much has already been discussed regarding the issue of electronic fund transfer fraud. Many merchants and banks consider it as part of the "price of doing business".[14]

The fax machine is considered by many to be an office staple. Indeed, the fax machine is considered to be a "revolutionary contribution to modern communications"[15]. It, too, is also vulnerable to high-technology crime. Law enforcement currently has the technology available to intercept fax transmissions from the sender to the receiver. This is a boost for law enforcement in that several criminal operations are using the fax as a communications medium for unlawful activities. Fax evidence can be electronically obtained via high-technology, and used against these criminals at a later time. But if law enforcement has this ability it is safe to assume that the criminals are not far behind.[16] Law enforcement needs to be aware that those same criminals also have the ability to intercept "their" fax transmissions too. What is law enforcement doing to protect its own communications fax networks? This question needs to be addressed and answered by all law enforcement agencies. A solution to this problem can be the application of encryption to fax communications. But encrypted faxes can be a double edged sword. The solution can also create a new nightmare for law enforcement in the future when criminals start encrypting their messages.[17]

Illegal criminal activity on the Internet computer network and computer bulletin boards have raised some significant concerns about the impact of high-technology crimes on millions of users. Internet-International alone, is a collection of 2.2 million corporations and government agencies and serves 20 million people.[18] Keith Strandberg believes that anyone with a computer, modem and telephone service can become a

"computer criminal". According to Strandberg "On-line crime runs the gamut of possibilities, from the trading of illegal material (phone card numbers, credit card numbers, etc.) to copyright infringement of software (software piracy), to harassment and stalking, to the trading of illegal sexual material, and everything in between".[19]

Critics state that Cyber Space is a wide open frontier similar to that of the wild west days.[20] What is law enforcement doing about this now? Can we afford to wait much longer?

Continuous Change

It has become evident, in the last two years, that advances in technology will continue to drive how high-technology crime will be investigated in the future.

In the October 1994 addition of Omni magazine an article was featured about a recent break through in magnetic fingerprinting. The article discusses the use of a simple magnetic reader device that identifies the unique fingerprints of objects containing magnetic recorded data. The unique magnetic fingerprints are the random characteristics of the magnetic trace elements of the magnetic source medium. This source medium could apply to objects ranging from charge cards, computer disks and old Beatles tapes to security entry cards, electronic passkeys into computer networks, and even wire taps. Each magnetic source medium has "unique" identifying properties similar in concept to human fingerprints. The article suggests the possibility of virtually eliminating "credit card fraud and counterfeiting (which costs the consumers, banks, and merchants more than $1 billion a year), eradicate industrial espionage, detect bootlegged magnetic recordings, and make it impossible for even the most nimble outlaw to pilfer information and penetrate protected networks"[21]. This type of technological advancement could have some significant applications for law enforcement in the investigation of this type of crime.

Conclusion

Data collected in the technical report indicates strongly that current methods of investigation will not work in the age of computer-related crime. Not only are the techniques that have been used in the past not applicable, but the personnel using those techniques are, at present, incapable by experience and training to make us of the methods now coming on line.

Medium-size law enforcement agencies must develop partnerships with other law enforcement agencies and the private sector in order to effectively investigate high-technology crime in the future. Most medium-size law enforcement agencies are limited in the number of qualified personnel who have a good understanding of computers and applications of high-technology. Research indicates that larger law enforcement agencies, including the FBI and the California Department of Justice, are also limited in their ability to properly investigate this type of crime.

Medium-size law enforcement agencies clearly need to utilize the "team " approach in investigating high-technology crime in the future. No single agency internally has the expertise to investigate the myriad of high-technology crimes. An individual agency may have personnel who have a good understanding of how IBM compatible personal computer systems operate and can investigate crimes involving that type of hardware. But the same agency would be at a loss investigating high-technology crimes involving mainframe or Apple computers because no one in their organization is familiar with the respective operating systems. In addition, their personnel will probably

need outside assistance in gaining access to information stored on a hard disk that has been pass word or encryption protected.

It will be very important for these medium-size law enforcement agencies to be aware of the resources available to them in investigating high-technology crimes. Organizations such as Search Group, the FBI, Computer Emergency Response Team (CERT), Carnige-Mellon Institute Pittsburgh and the High-technology Crime Investigators Association are available to assist local agencies with these types of specialized investigations. Investigative networks focusing in the area of high-technology crime investigation are also a viable solution that medium-size law enforcement agencies can explore.

Medium-size law enforcement agencies will continue to investigate high-technology crimes with traditional types of investigative techniques well into the year 2003. Law enforcement agencies need to continue to utilize proven investigative techniques when investigating high-technology crimes. These agencies have utilized their department computer gurus to take the lead in investigating these crimes and will continue to do so in the future. Law enforcement agencies should send this first generation of Cyber Cops to formal training in high-technology crime investigation. This will the first step in developing a solid foundation for future investigative expertise in the organization. Interview and interrogation skills of the trained investigator will continue to be an invaluable tool in these types of investigations. The use of informants and intelligence information (larger and more inclusive data bases) will also continue to be an important tool for the investigator.

The seizing and examination of evidence will continue to be the weak link in a medium-size law enforcement agencies ability to investigate high-technology crimes. These agencies may need to retain the services of an individual or organization that is trained in high-technology criminal forensics. This is an area that most medium-size, for that matter large, law enforcement agencies lack the expertise and resources to properly seize, secure and examine the inner workings of computers and high-technology devices.

The investigation of high-technology crime will continue to be a challenge for law enforcement in the future. The reduction of low technology crimes will bring about a higher number of high-technology crimes committed. Criminals, in the past,used gloves to get around leaving fingerprints at the crime scene. Criminals, in the future, will use computers to committ crimes hoping to leave no electronic evidence for investigators to find. Law enforcement must work with other organizations, public and private, in developing partnerships to properly investigate this type of crime in the future.

Endnotes

[1] Search Group, Computer Fraud and Theft by Computer, Presentation for the California Reserve Peace Officers Association Annual Conference, September 25-26, Sacramento, CA.

[2] Ibid.

[3] Deirdre Martin, "Fighting Computer Crime", Law Enforcement Technology, October, 1993, 82-84.
[4] Patricia A. Parker, "Downloading Computer Crime", Police, October, 1991, 55-57, 112-123.
[5] U.S., Department of Justice, Computer crime, Electronic Fund Transfer Systems and Crime, July 1982, v1.

[6] Patricia A. Parker, "Downloading Computer Crime", Police, October, 1991, 55-57, 112-123.

[7] Mark Lewyn, "Phone sleuths are cutting off the hackers; corporations and phone companies join to end long-distance fraud," Business Week, July 13, 1992, 134.

[8] Kristina B. Sullivan, "Virus policies vary widely: 600-plus viruses hit 63 % of PCs," PC Week, vol., December 9, 1991, 33.

[9] Jane Bird, "Inside track on hackers," Management Today, June 1992, 78.

[10] August Bequai, How to Prevent Computer Crime: A guide for managers, John Wiley and Sons, New York, NY, 137.

[11] Fred Cotton and William Spernow,
[12] Keith W. Strandberg, "Thin Blue Line Must Infiltrate On-line Criminals," Law Enforcement Technology, November 1993, 28-32, 51-52.

[13] Philip M. Stanley, "Computer Assisted Investigation Of Computer Crime", in Proceedings of the Sixth IFIP International Conference on Computer Security and Information Integrity in Our Changing World (Helsinki, Finland, 23-25 May, 1990), ed. Klaus Dittrich, Seppo Rautakivi, Junhani Sarri, 389-402.

[14] Richard D. Morrison, "Credit Card Fraud; Crime Does Pay," Law Enforcement Technology, October 1994, 94-97.

[15] Richard D. Morrison, "As a matter of Fax: The Fax of the Matter," Law Enforcement Technology, October 1994, 70-74.

[16] Richard D. Morrison, "As a matter of Fax: The Fax of the Matter," Law Enforcement Technology, October 1994, 70-74.

[17] Richard D. Morrison, "As a matter of Fax: The Fax of the Matter," Law Enforcement Technology, October 1994, 70-74.

[18] John Diamond, "Pentagon can't shake hackers: Intruders still gain access to unclassified computer file," Associated Press, reprint Sacramento Bee, 22 July 1994, A18.

[19] Keith W. Strandberg, "Thin Blue Line Must Infiltrate ON-On-line Criminals," Law Enforcement Technology, November 1993, 28-32, 51-52.

[20] Keith W. Strandberg, "Thin Blue Line Must Infiltrate ON-On-line Criminals," Law Enforcement Technology, November 1993, 28-32, 51-52.

[21] Linda Marsa, "High Tech Detecting: The case of magnetic fingerprints", Omni, vol. 17, no. 1, October 1994, 26.

Bibliography

Associated Press, "Hacker's racist message heats up Internet", Sacramento Bee, 19 October 1994.

August Bequai, Technocrimes. Lexington, Mass: Lexington Books, 1987

Jane Bird, "Inside track on hackers," Management Today, June 1992.

J. J. Bloombecker, "Short-circuiting computer crime," Datamation, vol. 35, October 1, 1989.

John Diamond, "Pentagon can't shake hackers: Intruders still gain access to unclassified computer file," Associated Press, reprint Sacramento Bee, 22 July 1994.

Search Group, Computer Fraud and Theft by Computer, Presentation for the California Reserve Peace Officers Association Annual Conference, September 25-26, Sacramento, CA.

William Spernow and Fred Cotton, personal interview, Sacramento, CA, 29 September 1994.

Mark Lewyn, "Phone sleuths are cutting off the hackers; corporations and phone companies join to end long-distance fraud," Business Week, 13 July 1992.

Linda Marsa, "High Tech Detecting: The case of magnetic fingerprints", Omni, vol. 17, no. 1, October 1994.

Deirdre Martin, "Fighting Computer Crime", Law Enforcement Technology, October, 1993.

Bill Montague and Philip Fiorini, "Privacy abuse "confirms the worst fear"," USA Today, 20 July 1994.

Richard D. Morrison, "Credit Card Fraud; Crime Does Pay," Law Enforcement Technology, October 1994.

Richard D. Morrison, "As a matter of Fax: The Fax of the Matter," Law Enforcement Technology, October 1994.

Patricia A. Parker, "Downloading Computer Crime", Police, October 1991.

Evan I. Schartz, Jeffrey Rotherfeder, Lewyn, "Viruses? Who are gonna call? Hackbusters (computer crime)," Business Week, 6 August 1990.

Philip M. Stanley, "Computer Assisted Investigation Of Computer Crime", in Proceedings of the Sixth IFIP International Conference on Computer Security and Information Integrity in Our Changing World (Helsinki, Finland, 23-25 May, 1990), ed. Klaus Dittrich, Seppo Rautakivi, Junhani Sarri.

Keith W. Strandberg, "Thin Blue Line Must Infiltrate On-line Criminals," Law Enforcement Technology, November 1993.

Kristina B. Sullivan, "Virus policies vary widely: 600-plus viruses hit 63 % of PCs," PC Week, vol., December 9, 1991.

U.S., Department of Justice, Computer crime, Electronic Fund Transfer Systems and Crime, July 1982.

TABLE OF CONTENTS

LIST OF APPENDIXES

LIST OF ILLUSTRATIONS

LIST OF TABLES

SECTION I: INTRODUCTION

Introduction

High-technology crime, also known as computer-related crime, currently does not have a standardized definition. The FBI, local legistration and the private sector have differing definitions of what high-technology crime entails. In both of the below listed definitions, it becomes apparent that high-technology crime encompasses a wide range of technological and legal applications.

Definition

The FBI defines computer-related crime as:

1. Computers as crime tools: "When criminals use computers as their tools, the crimes they engineer are essentially traditional crimes such as embezzlement, fraud and theft. The criminal uses a computer as an instrument like the forger's pen or the terrorist's bomb."[1]

2. Computers as crime targets: "This type of crime occurs when a company and the information it stores are the targets of a criminal act committed either intentionally by employees or externally by criminals. The external threat usually involves the use of telecommunications to gain unauthorized access to the computer system."[2]

Lawrence Young definition of computer-related crime includes the following general explanatory descriptions:

"1. Traditional larceny-related offenses. Includes the use of computer technology for theft of funds or other non-computer assets, and includes the related offenses of fraud and embezzlement

2. Intellectual property crimes. Includes the criminal infringement of trade [secrets] or [copyrights] that apply to computer programs, computer stored data, or equipment, whether or not a computer is used to accomplish such infringement.

3. Interruption of service or damage to computer assets. Includes all criminal acts resulting in the unavailability of timely computer use, whether due to the denigration of service time, complete disabling or alteration or equipment or programs, or destruction or alteration of data.

4. Theft of computer service. Includes the unauthorized use of a computer for any purpose, with suitable gradations of culpability and penalties depending on the value of the service used and whether outcomes included in category three(Interruption of service and damage to computer assets) are present in the commission of the crime.

5. Other traditional (non-larceny) criminal offenses. Includes the use of computers other than those described in category one (Larceny related).

6. Computer Espionage. Includes the use of computers in the acquistion of national secret or otherwisw classified material by means of obtaining computer data, whether or not those secrets are about programs or equipment.

7. Computer violation of privacy. Includes criminally infringing on individual privacy rights either by revealing or using information stored in or processed by a computer."[3]

His list also includes a definition of computer trespass. Computer trespass is fraudulently gaining entry or use of computers without authorization of the owner of the hardware or software, whether or not the entry into a computer system actually involves use or interruption of services, or other harms."[4]

For the purposes of this paper, high-technology crime will be defined as crimes committed through the use of computers, including but not restricted to related hardware and software issues and crimes committed against computers involving the use of advanced technologies. In this connection, the terms "computer-related crime" and "high-technology crime" will be considered as synonymous.

Background

In a 1993 article on computer-related crime, Fred Cotton and William Spernow reported an ever increasing variety of fraud and criminal acts being perpetrated by the use of computers. Cotton and Spernow also described several different aspects of high-technology crime. First, there are insider crimes, those that involve suspects who have legitimate access to a computer system but who exceed their authority and commit fraud, theft or vandalism. Second, they discuss how malicious hackers use tactics such as introducing computer viruses to debilitate computer systems. Last, Cotton and Spernow advise that computers are being used to commit crimes in the areas of

telecommunications fraud, child pornography,terrorism, computer contaminants and espionage.[5]

High-technology crime has been occurring for over the past two decades. The accounting firm of Ernest and Young estimates that computer-related crime has cost US businesses approximately $3 billion to $5 billion a year in losses.[6] Search Inc. reports that other researchers place the annual total loss as high as $40 billion if losses from viruses and software piracy were included. They also report that only 6% to 11% of computer-related crime is reported to authorities.[7]

According to J.J. Bloombecker money crimes of the past century such as bank robbery, million dollar armored car holdups and insurance fraud will seem inconsequential in the future when compared to high-technology crime. Bloombecker adds that computer crime costs businesses in America over $500 million a year.[8]

August Bequai reports that the "largest heist in US history, which was more than $2 billion, used a computer and not a gun." He also states that the private sector will spend a projected $100 billion by 1995 for security services and devices to protect themselves against fraud, terrorism and unauthorized electronic tapping.[9]

The use of bank cards to make electronic payments is now a way of life. The electronic manufacturing of counterfeit or altered cards will be a growing activity of organized and professional criminals.[10] One type of computer-based/high-technology crime that people are becoming more aware of stems from electronic fund transfer thefts from automated teller machines (ATM's). This crime typically involves the theft of funds by illegally gaining access to the account via stolen credit card and personal

identification number (PIN).[11] In 1982, Bureau of Justice Statistics maintained by the US Department of Justice stated their belief that electronic fund transfer fraud will become more prevalent in the future.[12] Search Group again states that US financial institutions transfer 1 trillion dollars a day over world wide electronic fund transfer computer networks.[13]

The Internal Revenue Service (IRS) has been one of the latest victim of high-technology crime. Senator John Glenn, chairman of the Governmental Affairs Committee, which oversees IRS stated that, "scam artists have use the IRS electronic income-tax filing system to bilk the government out of at least $1 billion a year." Over 13 million of 115 million tax returns were filed with the IRS electronically in 1993.[14]

William G. Flanagan and Brigid McMenamin discuss the cellular telephone industry's plight regarding these types of thefts. Computer hackers cost the cellular telephone industry over $300 million a year in losses because at the moment it is impossible to prevent these crimes. According to Mark Lewyn, A.T. & T, M.C.I. Communications Inc., and US Sprint are among several corporations that have taken steps to monitor long-distance usage. Lewyn adds that phone fraud losses for the industry estimated to run from $500 million to $4 billion per year.[15]

Donn Parker of S.R.I. provides a contrasting opinion regarding the dollar loss estimated by most high-technology industry experts. Parker believes that there are currently no accurate statistics available on estimating the cost of computer crime to society. Parker states that there are reported annual losses of computer-related crime which vary from $143 million to $41 billion. Parker concludes that this information is

not statistically valid because victims generally resist revealing loss information to law enforcement."[16]

According to Keith Strandberg computer crime will be the wave of the future because the children of the 1980's and 1990's have grown up with computers. He adds that this new generation,children of the 1980's and 1990's, will be as adept in using computers to commit crimes as were car thieves of the 1950's in using wire to "hot wire" cars.[17] Another source indicates that computer crime will tend to increase in proportion to the numbers of computers in use. There is little question that, with the numbers of computers increasing, so will computer-related crime.[18]

The private sector is also expressing a growing concern regarding who is going to investigate high-technology/computer-based crime in the future. Current data indicates that businesses can spend up to $1 million a year trying to protect themselves against hackers and computer viruses.[19]

Fred Cotton and William Spernow report that law enforcement administrators are not aware of a growing trend of criminals using computers to commit traditional crimes such as telecommunications fraud, child pornography, espionage, terrorism and other criminal activities. Cotton and Spernow state that their organization has been involved in a growing number of high-technology crime cases across the nation which computers are being used.[20] Another source indicates that law enforcement administrators are aware of well-publicized crimes such as computer-based fraud and electronic funds transfer thefts. The source suggests that they are probably not aware, however that industry experts

estimate over $4 billion are lost annually due to high-technology or computer-based crime.[21]

Bequai believes that law enforcement "lacks in a cohesive strategy" of what role each will have in these complex investigations. In addition, communications between the world of business and law enforcement are poor and need to be improved. He adds that the private sector believes that America's present law enforcement "is a patchwork of small, often inefficient police agencies working at odds with each other. Bequai also believes that private sector management must work together with law enforcement in properly investigating many types of computer crime.[22]

Cotton and Spernow conclude that local law enforcement agencies are going to have a difficult time investigating this growing crime problem because they lack computer literate criminal investigators and adequate technical resources.[23] Bequai suggests that law enforcement administrators develop strategies of what their department's role will be in investigating high-technology crime in the future.[24]

Issue Formulation

By using the information obtained from an environmental scan, POST personnel, periodical information and library research, a Futures Wheel was developed to aid in structuring the topic.

Issue

The specific issue that this Command College independent study project will focus on:

How will medium-size law enforcement agencies investigate high-technology crime by the year 2003?

The traditional mandate for law enforcement has been the investigation of criminal offenses using traditional management and expertise. In the future computer-related crime, due to its level of sophistication, may require a change in the traditional role of law enforcement because of the nature of that type of crime.

Sub-Issues

Three sub-issues were identified in the futures wheel process that should be considered as part of this independent study project.

What types of training will be necessary for medium-size law enforcement agencies to properly investigate computer crime by the year 2003?

Because of the nature of computer-related crime, traditional methods of crime investigation will be inadequate for the purpose. Law enforcement may have to upgrade its training and/or adjust its investigation methods in the area of computer-related crime in order to meet the crime challenges of the future.

What will be the relationship among the private sector, the educational community and law enforcement in investigating high-technology crime by the year 2003?

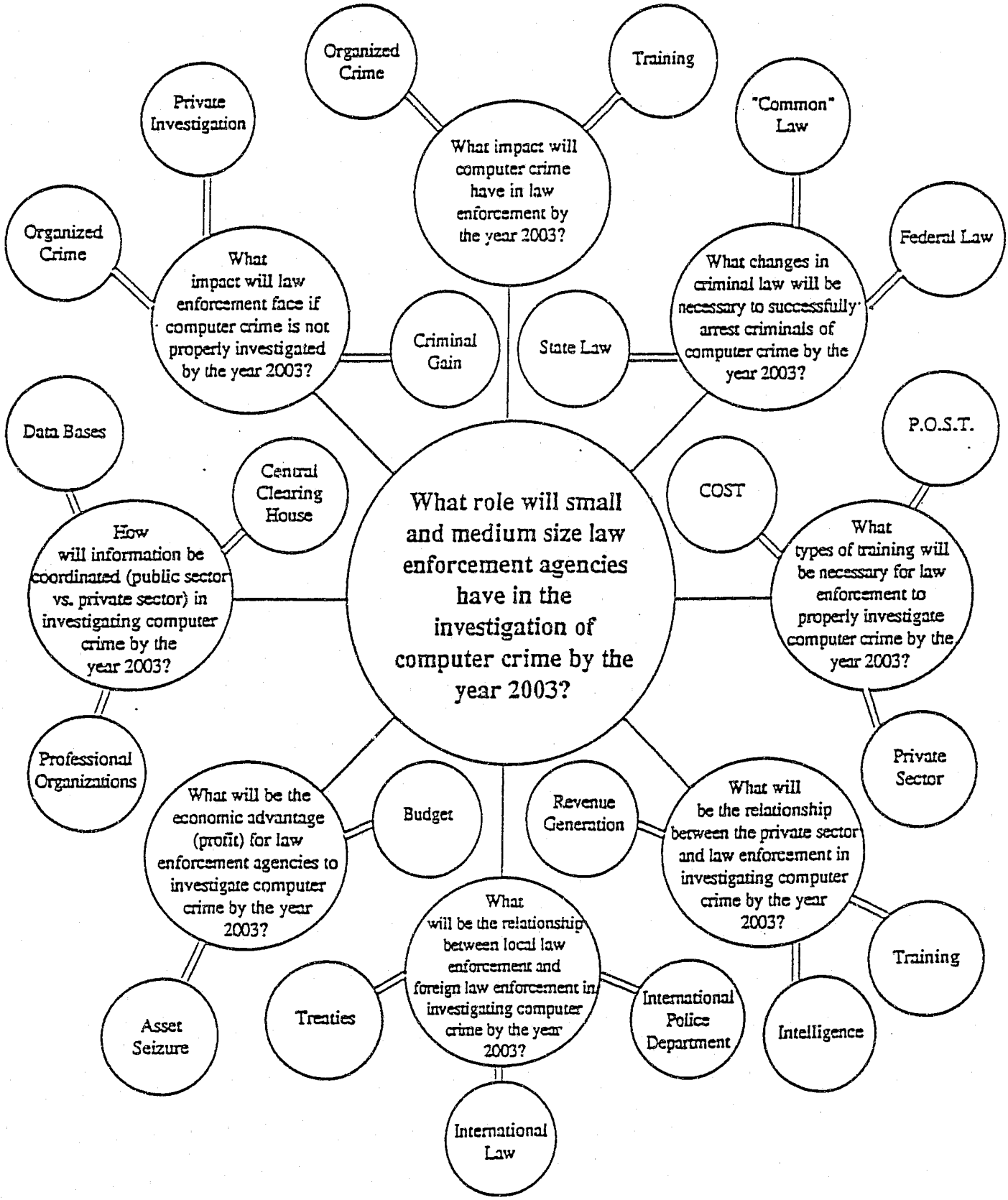
Given the facts of the intensely technical nature of computer-related crime investigation, it is possible that investigating computer-related crime in the future may bring about a synergistic relationship between law enforcement, the educational community and the private sector.

What level of criminal investigations will medium-size law enforcement agencies be responsible for in the investigation of high-technology crime by the year 2003?

Due to the sophistication and complexity of high-technology criminal investigations a different administrative approach may be necessary for medium-size law enforcement agencies.

In summation, it is this researcher's belief that the issue and sub-issues discussed in this paper represent futures concerns for a medium-size law enforcment agency into the twenty first century. Trends indicate that computer-related /high-technology crime will significantly impact law enforcement in the future.

Illustration #1
Futures Wheel



SECTION II: FUTURES RESEARCH

Futures Research

Methodologies

The issue question, How will medium-size law enforcement agencies investigate high-technology crime by the year 2003?, is futures oriented and will be impacted by trends and events that will occur in the next ten years. The use of the Nominal Group Technique by this researcher helped facilitate a look into that future.

Nominal Group Technique (NGT)

The Nominal Group Technique (NGT) is a process designed to facilitate a structured brain storming session which utilizes the anonymous inputting of ideas from invited subject matter experts. The NGT is primarily a small group exercise for achieving agreement on the answer to a single, usually complex question by a process that alternates private work with open discussion. It also allows panel members to both independently present their thoughts to the group and develop new ideas based on information generated by the panel.

A Nominal Group Technique Panel (NGTP) was selected by this researcher as a methodology to develop future trends and events regarding the issue question. Additionally, the NGTP also was charged with identifying the varying degrees of probabilities and magnitudes attached to those trends and events. It should be noted that the information derived from the NGTP provided the researcher with only a "snap shot" perspective of what the future would like five or ten years from now. The information

collected was based on the expertise, personality and perspective of the panel members on the day of the exercise.

The information developed and extrapolated from the NGTP was further analyzed utilizing an technique called cross-impact analysis. Cross-impact analysis is a method to measure the amount of impact that one event would have on other events if that event occurred.

Data collected from the cross-impact analysis along with other information accumulated during the course of this study were incorporated in the development of future scenarios for this project. From these scenarios, strategic and transition plans were written as a tool for law enforcement administrators to plan for the investigation of high-technology crime in the future.

Nominal Group Technique Panel Design

The Nominal Group Technique Panel (NGTP) consisted of members from both the private and public sectors. Careful thought and consideration was given in selecting the members of the NGTP. The NGTP was designed to be comprised of a broad spectrum of both professional and technical expertise from varying perspectives.

Nominal Group Technique (NGT) Panel

William Spernow, System Specialist in the Systems and Technology program with SEARCH group, Reserve Police Officer with Yuba City Police Department, recognized subject matter expert in high-technology crime investigations.

Dennis E. Pardini, manager of security and investigations for Quantum Corporation Milpitas, Ca. Background and experience in high-technology crime also extensive network with private sector security specialists.

Donald Ingram, Assistant District Attorney for Alameda County District Attorneys Office, supervising attorney for department's "high-technology crime team"; author, lecturer and instructor in computer-related crime and privacy issues. Past chairman of the Computer Science and Technology Section of the American Bar Association.

Ronald Carrera, Captain with the Sacramento Police Department, assigned to the Office of Administrative Services; Command College graduate; responsible for all computer-related security applications of the department.

Ronald Wilcynski, Special Agent with the Federal Bureau of Investigations assigned to the Sacramento office; specialist is the area of emerging telephone technologies and digital telephone; extensive training in areas of terrorism, electronic fund transfer fraud and national security issues.

Peter Martin, Supervising Investigator with the Yolo County District Attorney's Office; actively involved in the investigation of high-technology crime for the past eight years. Martin serves as his agency's lead in all computer-related applications.

Frank Quigley, Special Agent with the United States Secret Service; experienced in the investigation of high-technology crime.

Kevin Fairchild, President and Chief Investigator for Cyte-M, a firm that specializes in the investigation of high-technology crime. Fairchild is a retired officer from the Santa Clara Police Department.

Dale Lee, Senior Special Investigator assigned to the Special Investigations Bureau of the State Controller's Office; Specializes in the investigation of electronic fund transfer fraud.

Stephan Mick, member of the Computer and Communications Security Group for the Lawrence Livermore National Laboratory (LLNL), University of California; serves as the Computer Security Technical Support Team Coordinator; expert in handling attacks on computer systems and networks. Mick is also an expert in the management of computer security systems.

Jim McMahon, Sergeant with the San Jose Police Department; assigned to the Bureau Of Investigations; supervises the High-technology Detail responsible for the investigation of theft of trade secrets, computer fraud, technology transfer and forensic recovery of stolen/erased data from computers.

Trend Identification and Selection Methodology

Each NGTP participant was given documentation which contained a brief introduction to the NGT process prior to the meeting. Additionally, a detailed discussion regarding the differences between objective and subjective trends were discussed with the group prior to beginning the session.

The Nominal Group Technique panel originally developed 34 trends during its first round of discussion. The panel, through consensus, was able to combine several similar individual thoughts into one single trend statement. Additionally, there was a significant amount of discussion between various panel members which clarified their opinions regarding various trends. The Nominal Group Technique panel identified 10 trends which they felt would have an impact on the issue question.

Trend Definitions

Trend 1 **Criminal Law:** The level of Judges and Jurors understanding the complex nature of high-technology and computers.

Trend 2 **Criminal Investigations:** The level of investigation that medium-size law enforcement agencies are responsible for in the investigation of high-technology crime.

Trend 3 **Organized Crime:** The level of high-technology crime committed by organized crime on a global market.

Trend 4 **Crime Reporting:** The level of reporting computer-related crime to law enforcement by companies.

Trend 5 **Cyber-Cops:** The level of cooperative working relationships between the public and private sector investigators.

Trend 6 **Hackers:** The level at which organized crime will employ hackers to commit high-technology crime.

Trend 7 **Computer Crime Victims:** The level of vulnerability to high-technology crime of local businesses.

Trend 8 **Jurisdictional Boundaries:** The level of cooperation among law enforcement agencies with mutual legal jurisdiction.

Trend 9 **Rapid change:** The level of high-technology change that law enforcement must keep up to date.

Trend 10 **Computerized Information:** The level of criminal or unethical activity in the use of confidential data bases.

Trend Evaluation

The Nominal Group Technique panel was asked to forecast the trend levels given a set criteria. The criteria given to the panel were based on today being an arbitrary number equal to 100. Any value less than today would be less than 100 and any value more than today would be greater than 100. The panel was also asked to estimate the past (five years prior to today) and provide future estimates (5 years from today and 10 years from today).

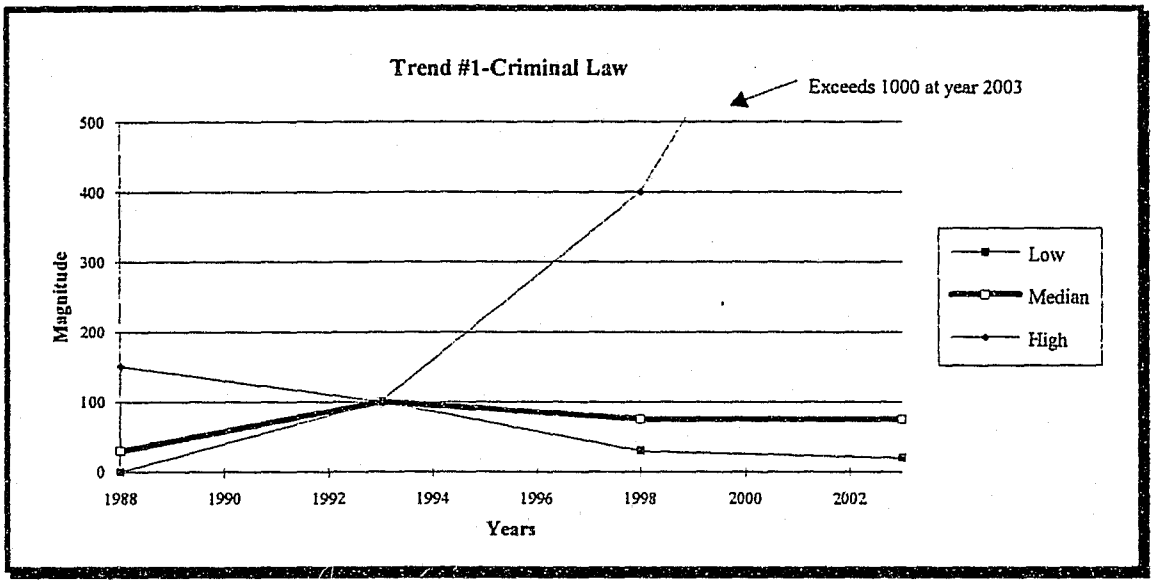
Table 1

Trend Evaluation

Trend #	TREND STATEMENT	LEVEL OF THE TREND * (Today = 100)			
		1988	Today	1998	2003
1	Criminal Law	150H 30M 0L	100	400H 75M 30L	1000H 75M 20L
2	Criminal investigations	125H 70M 0L	100	200H 100M 30L	200H 100M 150L
3	Organized Crime	60H 10M 0L	100	300H 150M 60L	600H 200M 80L
4	Crime Reporting	50H 10M 0L	100	200H 125M 20L	500H 150M 50L
5	Cyber-Cops	50H 5M 0L	100	200H 200M 40L	1000H 250M 80L
6	Hackers	60H 20M 1L	100	300H 150M 50L	800H 180M 80L
7	Computer Crime Victims	80H 25M 0L	100	500H 150M 60L	1000H 200M 90L
8	Jurisdictional Boundaries	70H 20M 5L	100	400H 150M 30L	800H 200M 40L
9	Rapid Change	200H 30M 0L	100	300H 100M 40L	500H 100M 60L
10	Computerized Information	60H 40M 0L	100	200H 150M 50L	650H 160M 80L

Panel medium N=12

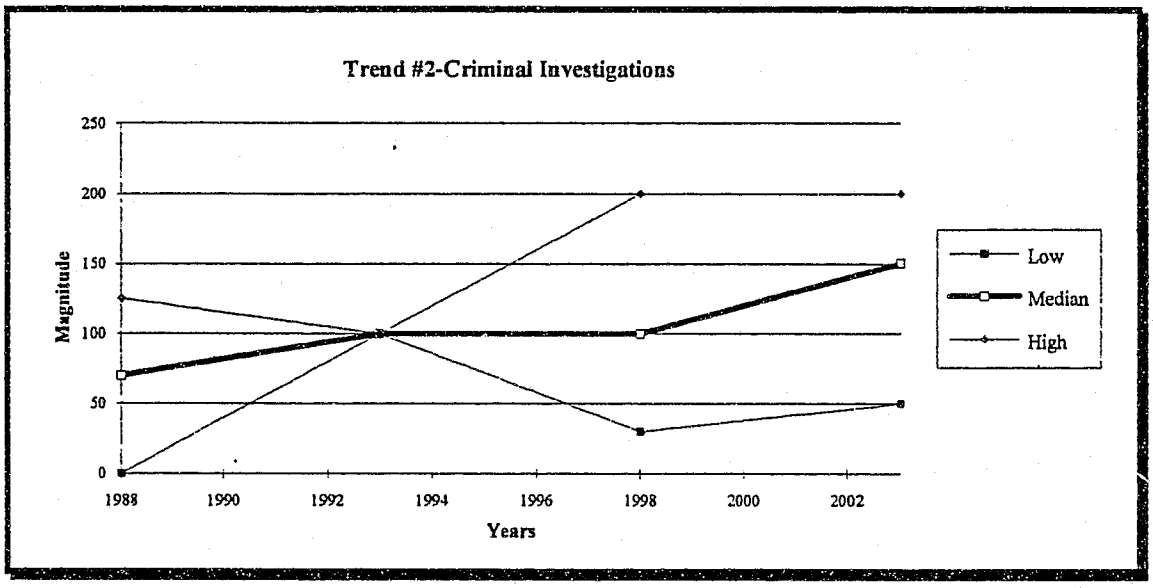
Illustration #2



Trend 1 **Criminal Law:** There was a considerable amount of discussion among panel members regarding the ability of judges and jurors to comprehend the complexities of high-technology crime and the criminal law associated with it. The unusually high forecast was based on the supposition that a majority of the panel members felt that society as a whole was gaining a better understanding of computers. This was primarily due to the fact that more and more people are using computers daily and that technological change was becoming an important part of their lives. The low forecast of the panel represents a view that technology was evolving at such a rapid rate and very few people fully understood it because of its inherent complexities. The median forecast denotes the consensus the group believed in regarding the successful prosecution of high-technology crime could be compromised by the lack of understanding and knowledge by judges and jurors in this arena. The panel discussed the development of educational

seminars for judges, prosecutors and prospective jurors to heighten their awareness of high-technology to criminal applications.

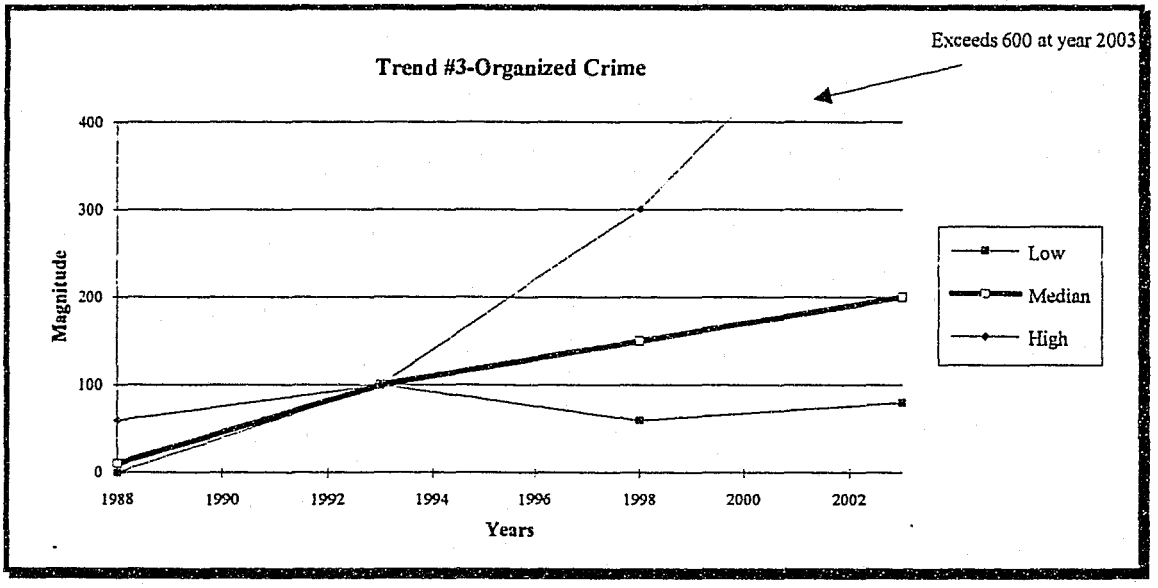
Illustration #3



Trend 2 **Criminal Investigations:** The panel was very concerned with the quality of criminal investigations conducted by law enforcement agencies in the area of high-technology crime. The high forecast suggests that panel members felt that medium-size law enforcement agencies were more capable of conducting investigations involving high-technology crime five years ago than today. The panel's scores were based on the opinion that the level of sophistication used by criminals in the arena of high-technology crime was still in its infancy. The panel also felt that many of the high-technology crimes committed followed traditional crime paths such as thefts, frauds, and embezzlements.

The low forecast was based on it's feelings that law enforcement did a poor job of investigating high-technology crime five years ago. It felt that law enforcement was ill prepared to deal with high-technology crime five years ago and the same will hold true in the future. This was principally because both criminal investigators and law enforcement administrators failed to comprehend the gravity of high-technology crime in the future. Those investigators and administrators who understand the future problems associated with high-technology crime are frustrated by both a lack of resources and training to effectively meet tomorrow's challenge. It was also interesting to note that the median score tends to indicate that law enforcement will neither improve nor get worse in investigating high-technology crime in the future.

Illustration #4

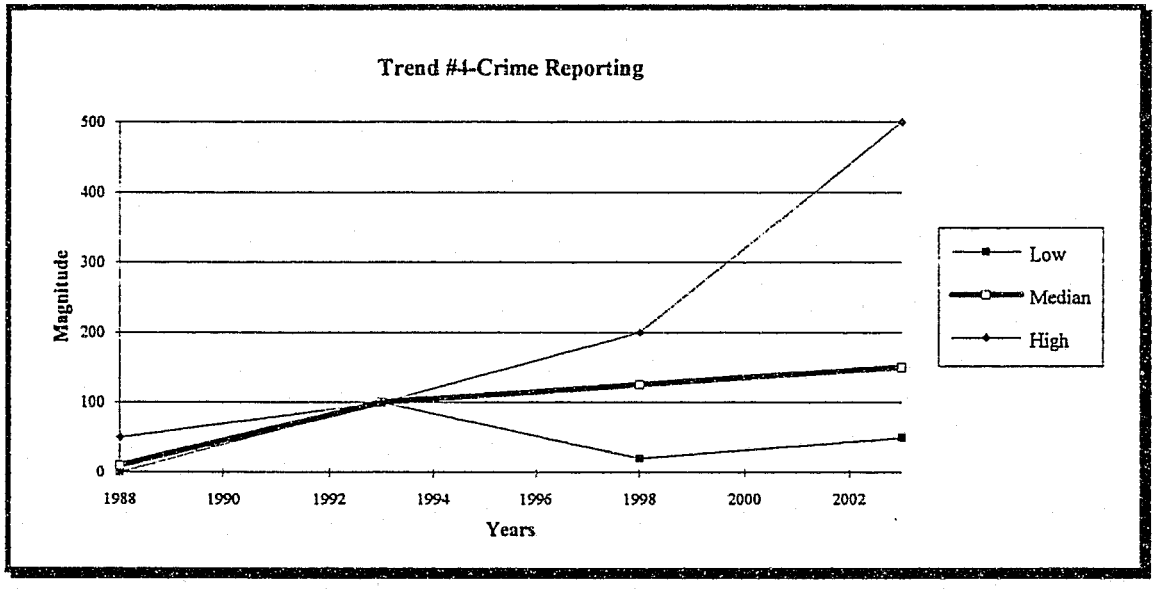


Trend 3 **Organized Crime:** The panel voiced a growing concern regarding organized crime becoming more involved in the high-technology crime area. The high

forecast level was based on the panel's opinion that law enforcement has been fortunate up to this point because organized crime has not been heavily involved with high-technology crime. The data strongly suggests that the level of their involvement in high-technology crime will expand in the future because of the tremendous profits associated with this type of criminal activity.

The median forecast was based again on the premise that high-technology crime can bring millions if not billions of dollars to organized crime families by means of electronic fund transfer fraud and other illegal applications of futures technologies. They predicted that it was inevitable that organized crime families in the future will become heavily involved with high-technology crime.

Illustration #5

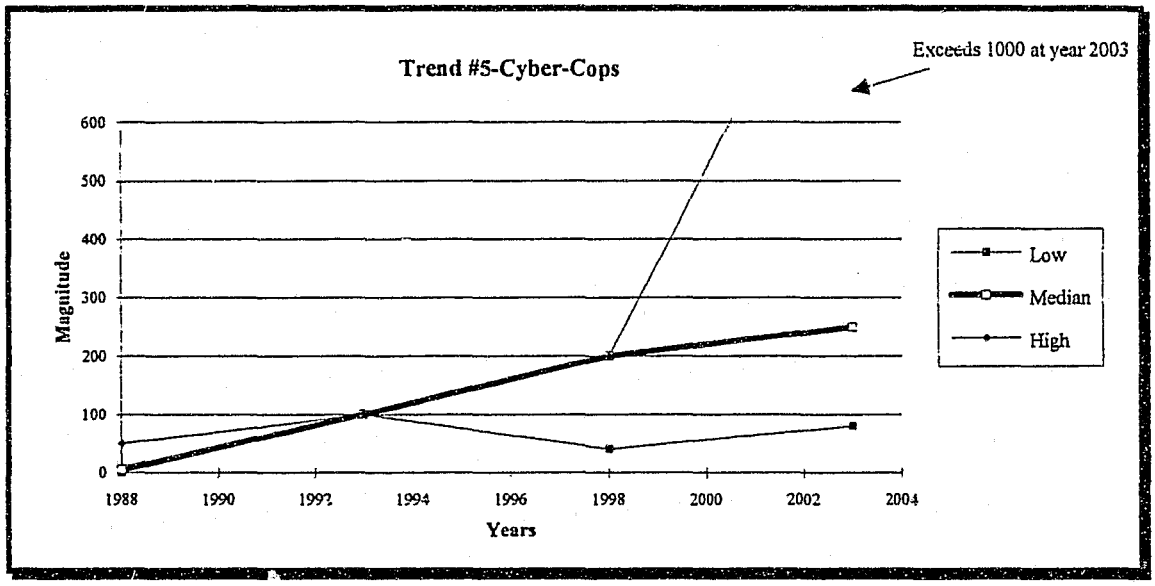


Trend 4 **Crime Reporting:** The panel had diverse views on the issue of companies reporting high-technology crimes to law enforcement. Overall, it was the

consensus of the group that high-technology crime was significantly under reported by the private sector today. The high forecast was based on a projected growing awareness and commitment of law enforcement to properly investigate high-technology crime. This would bolster the private sector's confidence in law enforcement's ability to properly investigate computer crime and thus enhance reporting. The median forecast was primarily driven by law enforcement improving its ability to investigate high-technology crime violations because of mandated reporting suggested by one panel member. The low forecast was based on the opinion that the private sector would hesitantly report this type of crime at a lower level due to fear that the public would lose confidence in their company. The private sector also lacked confidence in law enforcement's ability/desire to investigate this type of crime

The median tends to support the premise that companies will increase their reporting of computer crime at a level far behind the actual crime rate.

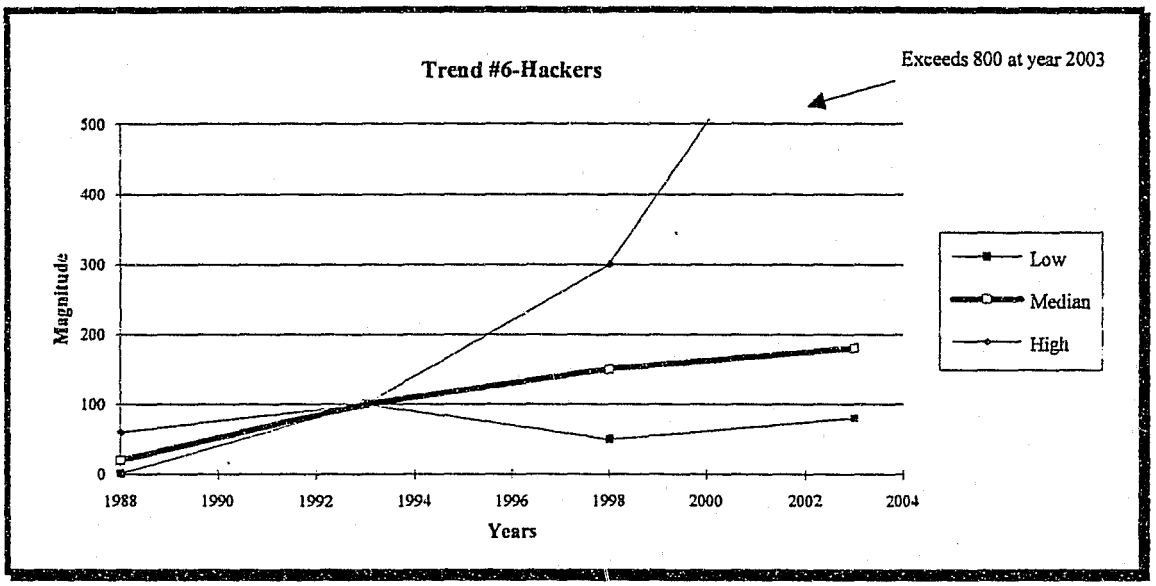
Illustration #6



Trend 5 **Cyber-Cops:** Of the 10 trends that the panel identified, Trend 5's median forecast was the highest of the group. The panel felt strongly that there needs to be a dynamic relationship between the public and private sectors regarding the proper investigation of high-technology crime. The high forecast was based on the premise that law enforcement does not have the proper training, education, funding and equipment to investigate high-technology crime without the active participation of the private sector. The median forecast was based on partnership models currently being used by the San Jose Police Department and the FBI. The low forecast was driven by the collective opinion that the private sector companies felt that they had to investigate high-technology crime themselves either because of law enforcement's lack of interest or capabilities. It was strongly suggested by a consensus of panel members that law enforcement begin to

develop investigative partnerships with private sector high-technology companies in investigating high-technology crime.

Illustration #7

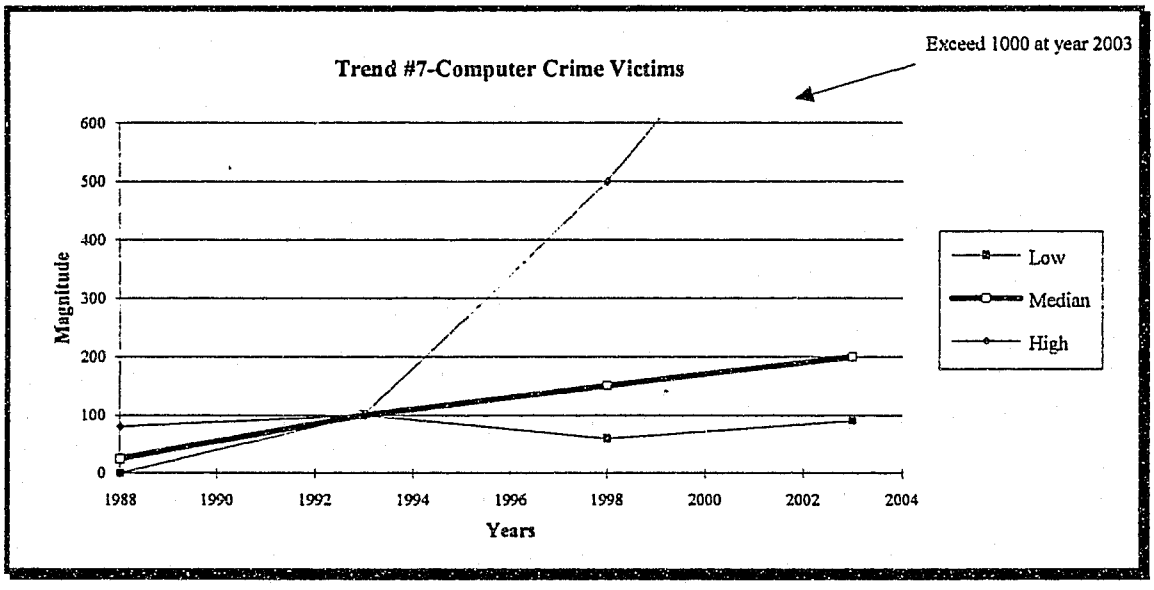


Trend 6 **Hackers:** The panel felt that there would be a trend for illegitimate businesses and organized crime families to employ computer hackers to commit high-technology crimes in the future. The high forecast was based on the panel's opinion that several private sector companies already employ hackers who have broken into their computer systems as security experts to prevent others from doing the same. Other panel members argued that many computer hackers are more capable than company computer programming experts. The median forecast was based on the premise that the Nintendo generation is in our colleges today and this will cause a growth in the numbers of hackers in the computer community. This new generation of hackers will seek and get

employment in government and legitimate business thus stemming the tide of the criminal hackers.

Other panel members suggested that law enforcement entertain the notion of hiring hackers as consultants in assisting them in the investigation of certain cases. There was consensus among the panel that hackers will play a significant role in high-technology crime in the future.

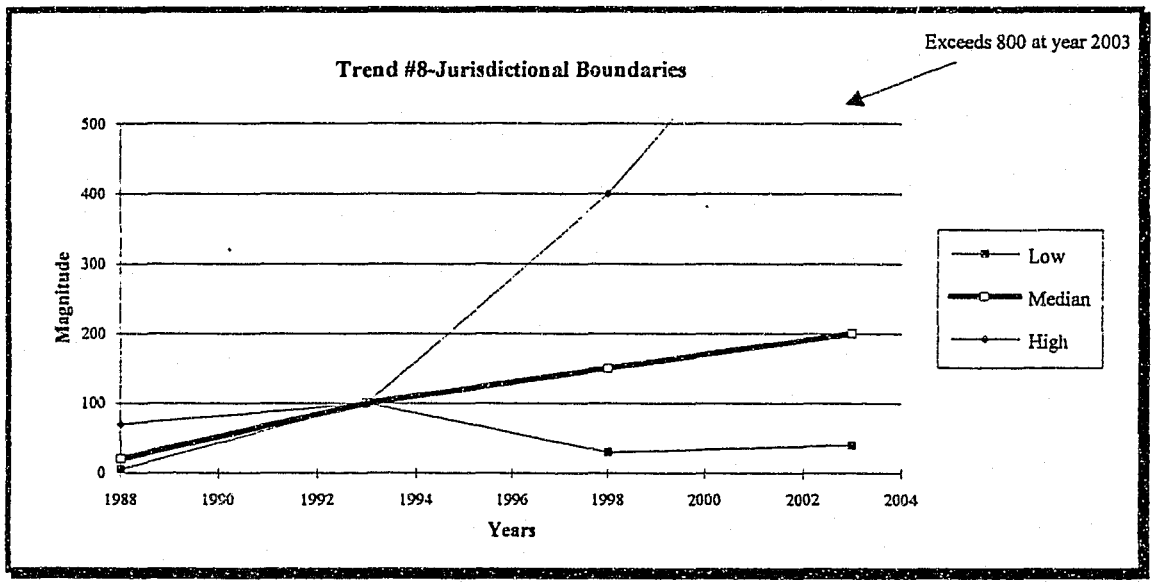
Illustration #8



Trend 7 **Computer Crime Victims:** It was the consensus of the panel that local businesses will become more vulnerable to high-technology crime in the future. The extremely high forecast was largely driven by the fact that more and more businesses are using computers in their daily activities such as: electronic fund transfers(bank cards/credit cards), check fund verification, credit verification and inventory systems. They felt that the increased dependence on computer systems lends itself to greater

vulnerability to theft, fraud, and corruption. The median forecast was based on the level of high-technology crime currently being reported nationally and internationally by financial institutions. The low forecast was based on the opinion that there could be a decrease in the level of vulnerability of high-technology crime to businesses through improved security systems such as retina identification access systems.

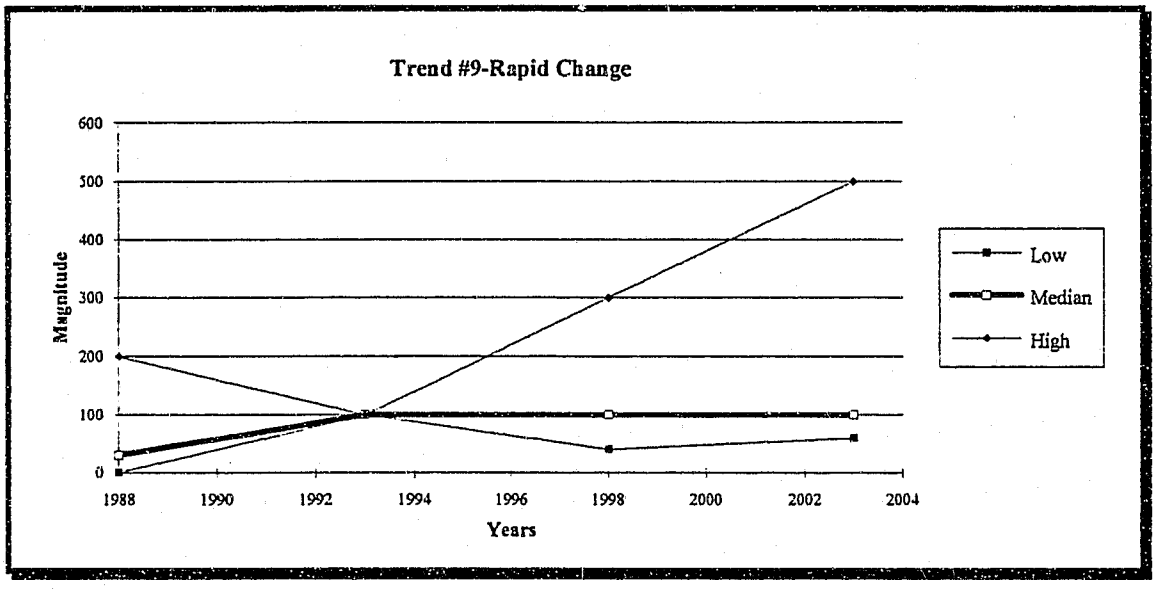
Illustration #9



Trend 8 **Jurisdictional Boundaries:** Again, the panel was unanimous in its agreement that jurisdictional boundary issues for high-technology crime can pose some interesting legal issues for law enforcement. The unusually high forecast was driven by the belief that with the onset of the personal computer/modem high-technology crimes can be committed by anyone and anywhere in the world. The median forecast was based on the levels with which local, national and international high-technology crime is

occurring today. The panel members were acutely aware of the jurisdictional boundary concerns for law enforcement with high-technology crimes.

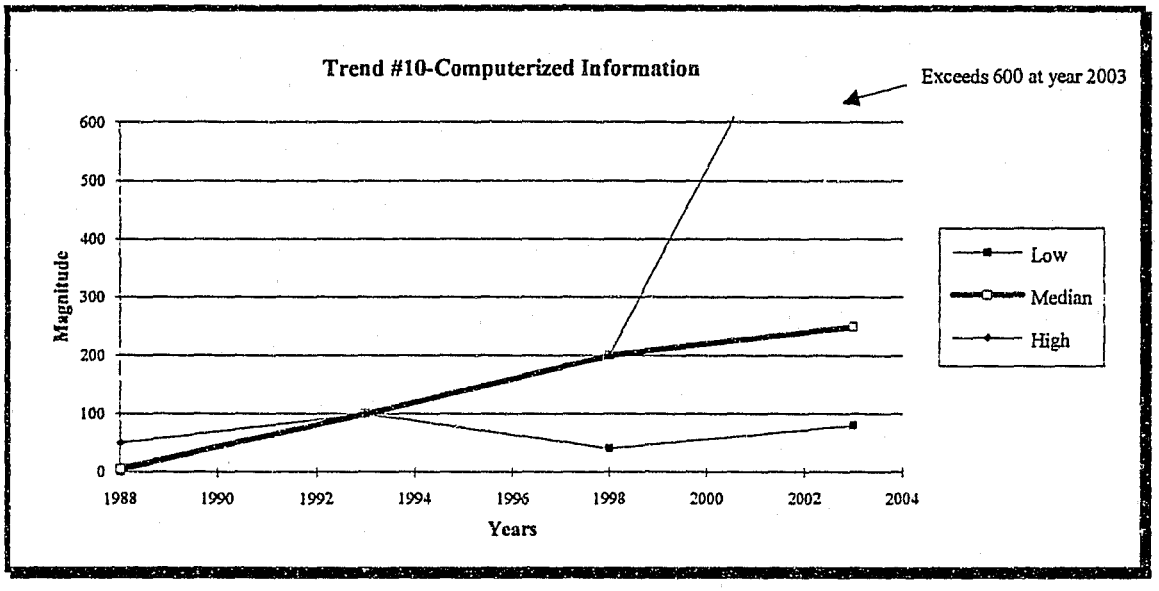
Illustration #10



Trend 9 **Rapid Change:** The panel discussed impacts of the ever-evolving rapid rate of change that is occurring in the area of high-technology crime. It felt that it was imperative that law enforcement not only keep up with those changes but try to be one step ahead of the criminals.. Panel members forecast that the level of high-technology change will be as great as 5 fold in the next 10 years. It was the panel's consensus opinion that the amount and type of change is difficult to predict given the nature of the subject matter The high forecast scores are primarily due to the end of the cold war with the USSR and how fast technology has evolved in the past 10 years. The panel predicted that classified military technology will be declassified and converted to civilian

applications, thus speeding up change. The median scores seem to indicate that law enforcement will maintain similar levels of knowledge within the next 10 years.

Illustration #11



Trend 10 **Computerized Information:** The illegal use of confidential data bases for criminal or unethical use will become more wide spread in the future according to the panel. The median score was based on the fact that individual data based information systems are growing at a rapid rate. The low forecast focuses on the assumption that criminals will not become as computer sophisticated over the coming 10 years. The high forecast represents the panel's opinion that criminals will take advantage of the vast amounts of information available and profit illegally from it.

Event Selection and Identification

The NGT panel was next asked to use the same process (same as the trend selection and identification) to determine 10 events that would most likely would impact the issue and sub-issues presented in this paper. A brainstorming session was facilitated by this researcher in which 38 events were identified by the NGTP. **See Appendix D.** Again the panel, through consensus, was able to combine several individual thoughts into one single event statement. As with the trend evaluation, all voting regarding event ranking was conducted in an anonymous manner through secret balloting.

Event Evaluation

After the NGTP completed their ranking of the top 10 events they were next asked to make a series of forecasts involving those events. These forecasts were to be based on their individual knowledge and expertise of the subject matter that was discussed at the NGT. A rating chart was provided to each panel member to record their opinions.

The panel next estimated the magnitude of impact each event would have on the issue and sub-issues if that event were to take place. A rating scale from 0 to 10 was used by each panelist to rate both the positive and negative impact for each event. The panel was also asked to forecast the probability of the occurrence for each event "Five Years From Today" and "Ten Years From Today". The panel was instructed to assign a number from zero (0) to one hundred (100) percent which would reflect the

probability of that event occurring. The panel was then asked to forecast which year the probability of each event's occurrence would exceed zero (0).

Event Definitions

Event 1 **Investigating High-technology Crime:** Law enforcement agency only investigates crimes only against persons and refuses to investigate crimes involving the use of high-technology.

Event 2 **High-technology Crime Committed:** A medium-size law enforcement agency fails to recognize a serious high-technology crime committed causing public criticism and embarrassment to the organization.

Event 3 **Law Enforcement Partnerships:** Several small agencies combine resources to offset costs of high-technology crime investigations.

Event 4 **Terrorist Attack:** Terrorists infiltrate and disrupt country's air traffic control computers system causing service disruption and loss of life.

Event 5 **Smart Cards:** Smart card replaces credit cards and currency as legal tender.

Event 6 **Entry Level Skills:** Legislation passed requiring high-technology crime investigation skills taught at basic police academies.

Event 7 **New Legislation:** Legislation is passed increasing the penalties for crimes involving use high-technology

Event 8 **Private Funding:** High-technology company funds computer training for mid-sized police department personnel.

Event 9 **Personal Communicator Number:** Personal Communicator Number (PCN) for telecommunications use (number can access user anywhere in the country) made available by phone companies.

Event 10 **State Computer Sales Tax:** Large additional tax on retail computer sales to fund high-technology training for law enforcement.

Table 2

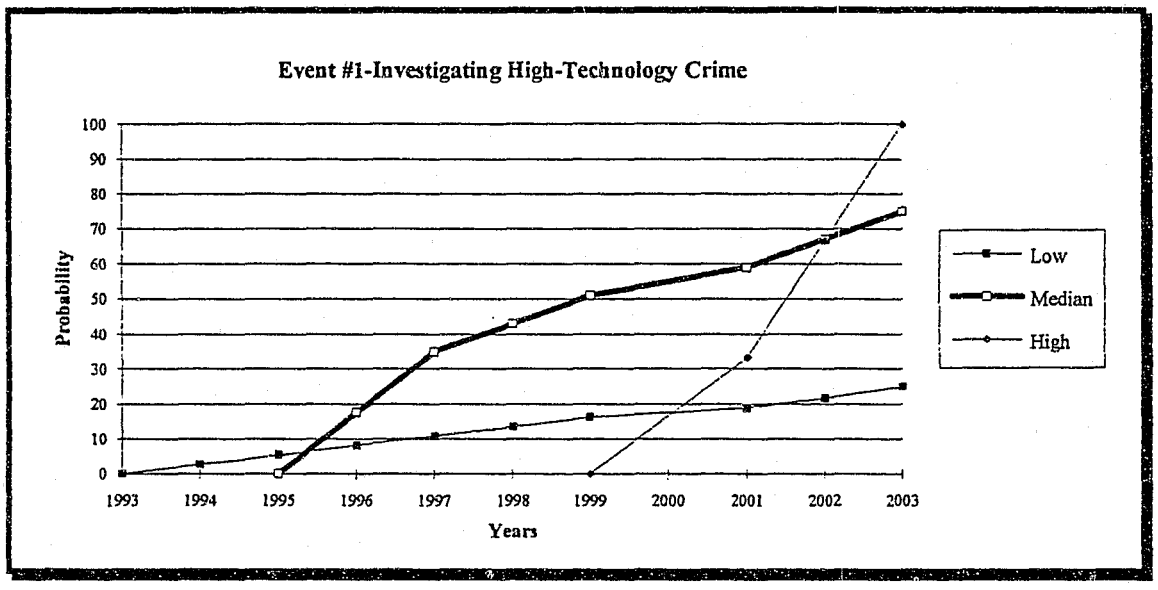
Event Evaluation

Panel Medians N=12

EVENT STATEMENT	* YRS UNTIL PROBABILITY FIRST EXCEED ZERO	PROBABILITY		* IMPACT ON ISSUE IF THE EVENT OCCURRED	
		5 YEARS FROM TODAY (0-100%)	10 YEARS FROM TODAY (0-100%)	POSITIVE (0-10)	NEGATIVE (0-10)
E-1 Investigating High-technology Crime	10L 3M *H	70H 30M *L	100H 70M 25L	8H 6.5M 0L	10H 6.5M 0L
E-2 High-technology crime committed	1L 1M 1H	100H 80M 20L	100H 80M 20L	5H 0M 0L	10H 9M 5L
E-3 Law Enforcement Partnerships	6L 4M 0H	80H 50M *L	100H 65M 30L	10H 0M 0L	10H 10M 0L
E-4 Terrorist Attack	10L 5M 1H	70H 40M *L	100H 80M 20L	10H 5M 0L	7H 5M 1L
E-5 Smart Cards	10L 5M 2H	85H 35M *L	100H 75M 10L	10H 10M 4L	8H 0M 0L
E-6 Entry Level Skills	10L 5M 1H	80H 30M *L	100H 70M 30L	10H 8.5M 5L	4H 0M 0L
E-7 New Legislation	10L 2M 1H	80H 50M *L	100H 90M 10L	10H 8M 8L	9H 2.5M 0L
E-8 Private Funding	10L 5M 3H	100H 50M *L	100H 75M 25L	10H 2.5M 0L	10H 5M 0L
E-9 Personal Communicator Number	10L 5M 2H	80H 20M 0L	100H 40M 0L	10H 10M 2L	10H 1M 0L
E-10 State Computer Sales Tax	10L 3M 1H	100H 65M *L	100H 90M 40L	10H 10M 1L	10H 1M 0L

* Scores outside rating criteria

Illustration #12

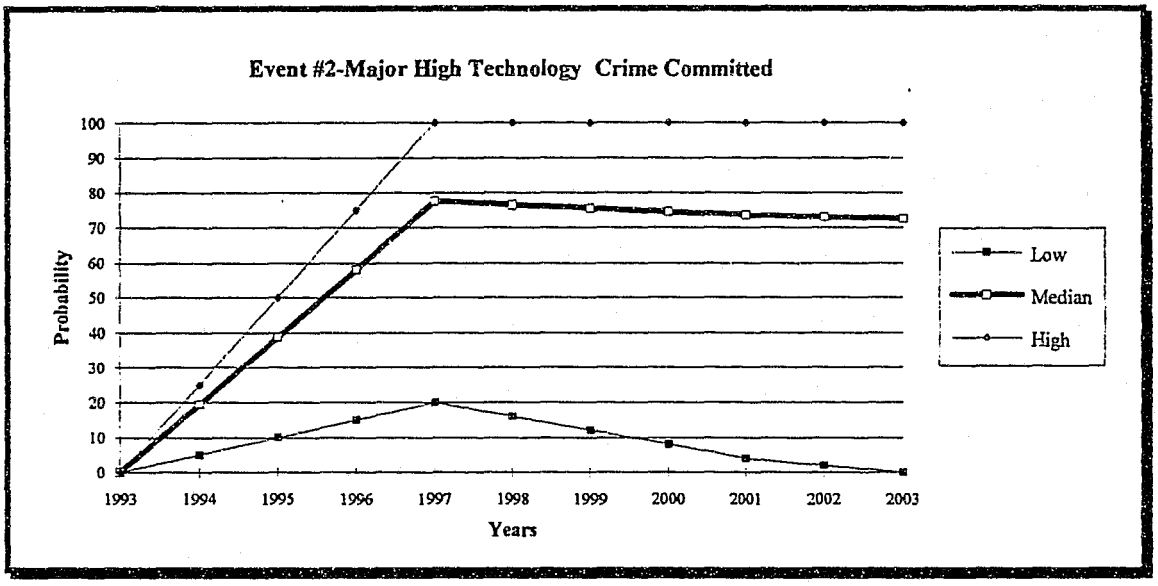


Event 1 **Investigating High-technology Crime:** The median forecast indicates that law enforcement agencies will continue to investigate significant crimes that occur in their jurisdictions well into the year 2003 at the cost of not investigating high-technology crime cases. The panel felt that due to budget reductions and the down sizing of many organizations high-technology crime investigation would take a back seat to the investigation of crimes against persons. The panel also weighed the negative impacts of law enforcement only investigating crimes against persons. It was the panel's opinion that if law enforcement investigated only these types of crimes that it would have a negative impact on the public's perception of police operations in general.

The asterisk on Table 2 denoting the low range for number of years until the probability first exceeds zero and 5 years from today was caused by a panel member who did not follow instructions.

The high forecast represents the panel's opinion that if current crime trends continue there will be a higher probability that law enforcement agencies will continue to have minimal resources and support to investigate high-technology related crime.

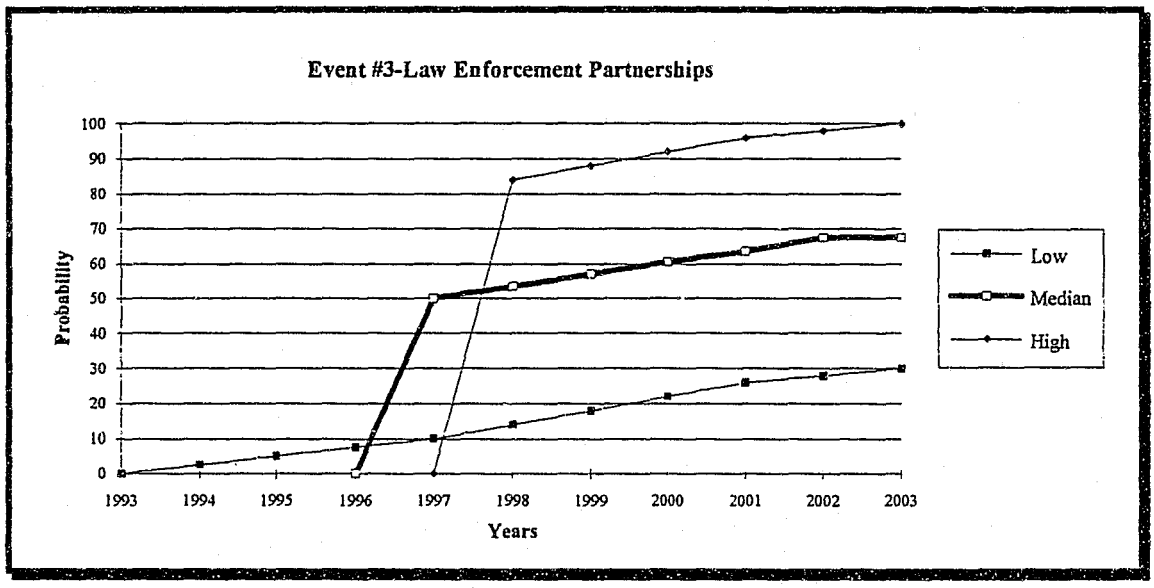
Illustration #13



Event 2 **Major high-technology crime committed:** The graph illustrates a high probability in the next 5 years that a medium-size law enforcement agency would fail to recognize a major high-technology crime committed causing public criticism and embarrassment to the organization. A majority of the panel members were grouped around the median level and felt that this type of adverse public reaction might prompt administrators to channel resources to address the problem. The median graph also denotes a slight reduction in the probability of the event occurring in the 10th year. The panel projected that a trend similar to Event 2 would stimulate small and medium-size law enforcement agencies to develop internal resources and expertise in the high-

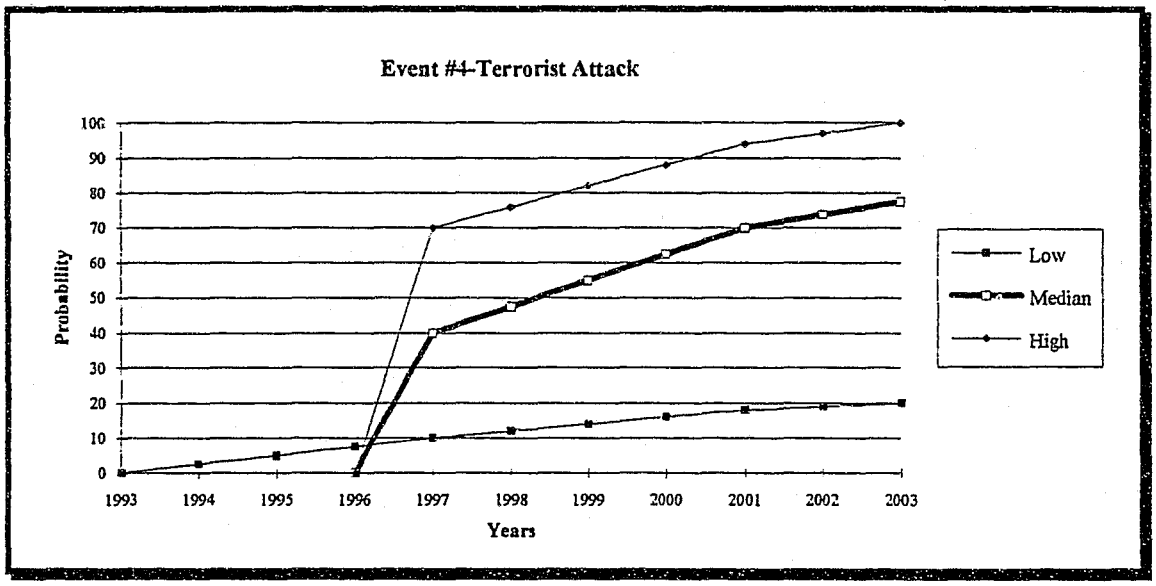
technology crime area. The panel strongly felt that if this event was to occur it would have a significant negative impact on the organization.

Illustration #14



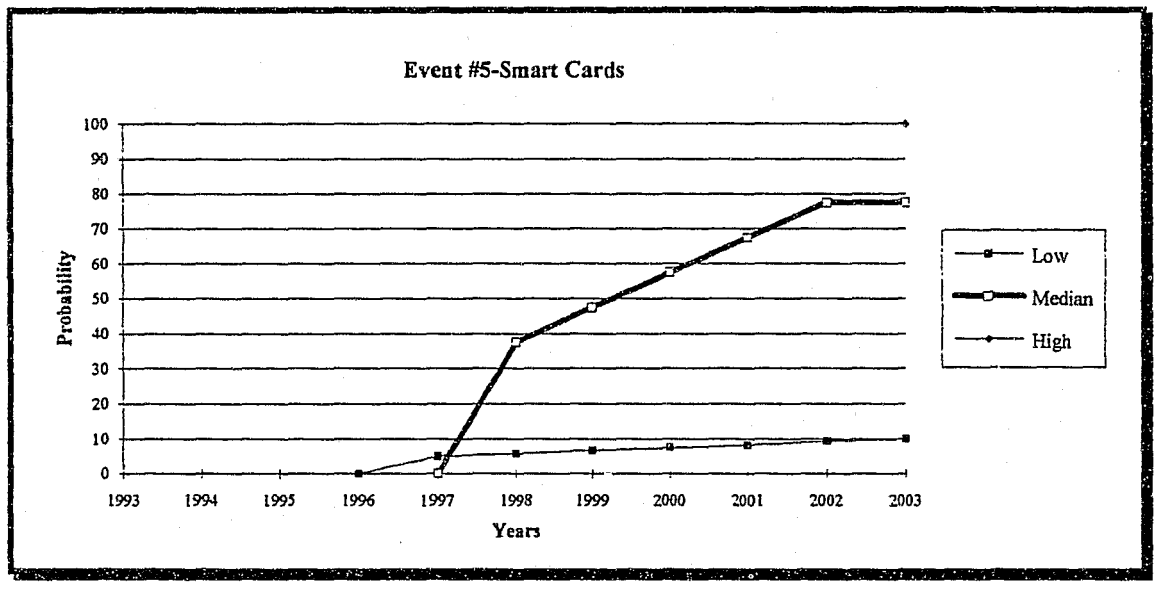
Event 3 **Law Enforcement Partnerships:** The graph indicated that the median forecast of the panel felt that there was a moderate probability of medium-size law enforcement agencies networking together to better investigate high-technology crime. There was a significant difference of 30 points between the median and high probability. Several members of the panel argued strongly that it made good sense for small and medium-size law enforcement agencies to join together and form partnerships that would be of mutual benefit to all parties.

Illustration #15



Event 4 **Terrorist Attack:** The graph indicates that there is a relatively low probability of a terrorist group using high-technology for terrorist activities within the first 5 years of the study. However, the graph also indicates that the probability of this event occurring in the second 5 years increases by 60 to 80 points. This was based on the panel's knowledge of the poor condition of the country's air traffic computer system. The FAA's air traffic control computers are antiquated and some equipment still uses vacuum tubes. The system lacks sophisticated security systems to protect it from this type of high-technology crime. The low forecast represents several panel member's opinions that there is a small probability that terrorist would have the sophistication to commit this type of high-technology crime.

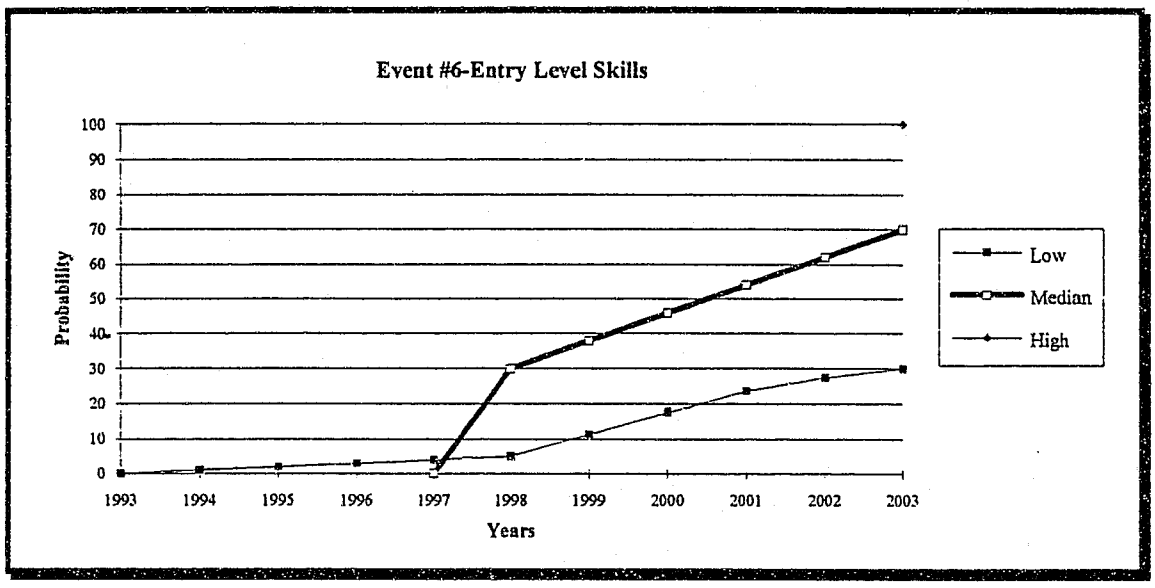
Illustration #16



Event 5 **Smart Cards:** There was a considerable amount of disagreement among panel members about electronic smart cards replacing currency as legal tender in the United States. As the graph illustrates, there was a significant difference between the low forecast and the median forecast. The difference ranges from 30 to 70 points. What was not represented on the graph was the high forecast. The high forecast was not represented because several panel members projected the 1st year of occurrence after the 10th year of the sample. Those ungraphed high forecast scores did skew the appearance of the median graph (would have been considerably lower). Several panel members scored the event first occurring 12 to 17 years from today. They were asked why they scored the event outside of the given perimeters. They felt that the probability of this event occurring within the 10 year time frame was extremely remote and not realistic.

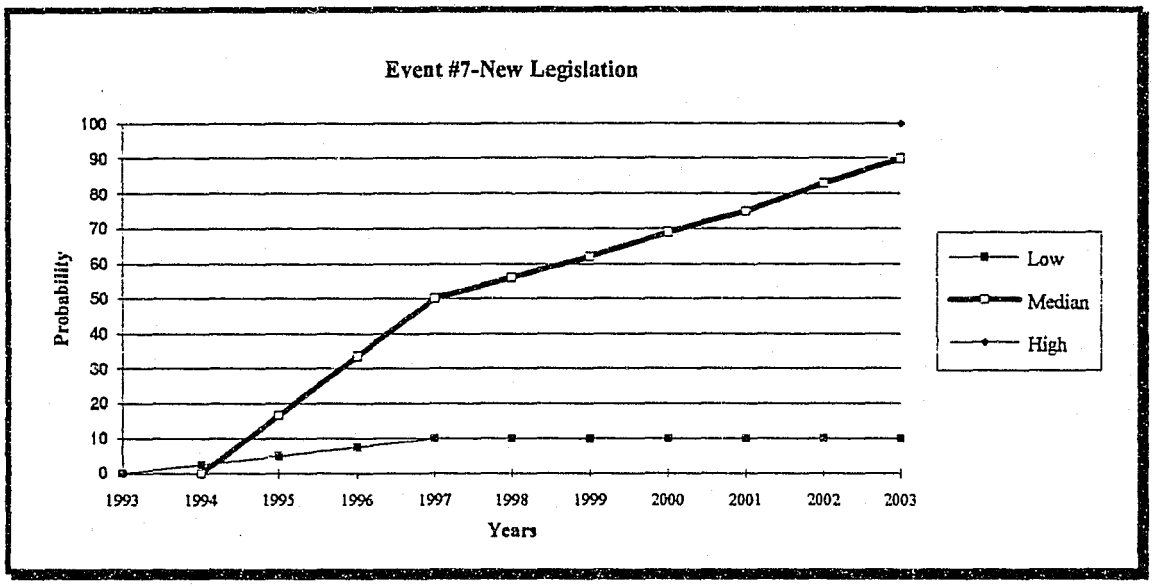
The low forecast was more representative of the panel's opinion that there was a low probability that this event would occur.

Illustration #17



Event 6 **Entry Level Skills:** The high forecast levels were not illustrated in this graph due to several panel members projecting the first year of occurrence after the 10th year of the sample. The median graph incorporates the high forecast data and was skewed. The median forecast should reflect a lower probability of the event occurring. Panel members felt that it was a good idea to incorporate high-technology crime investigation skills in the basic police academy. The panel strongly felt that it would be highly unlikely that the legislature would pass a law that would require the subject matter to be taught at the academies. Again, the low forecast was more representative of the panel's opinion on the issue. It felt that there was a low probability of the event occurring.

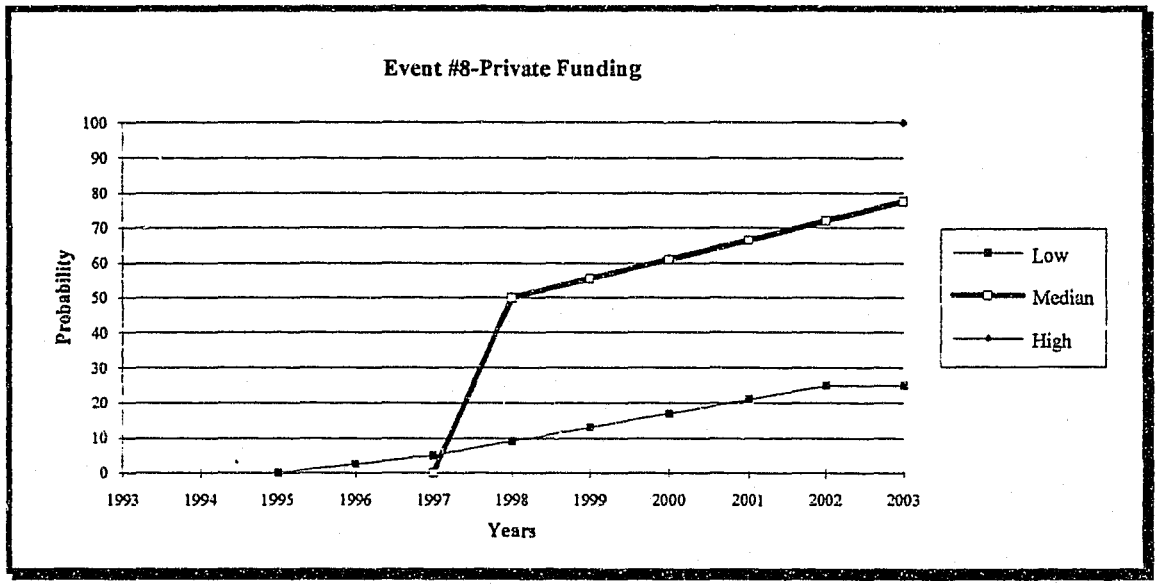
Illustration #18



Event 7 **New Legislation:** The graph illustrates the median forecast for the probability of new legislation to be passed in the next 10 years increasing the punishment for the use of high-technology in crime. The median curve was skewed by several panel members projecting the first year of the event's occurrence 20 years after the maximum end point of 10 years. This created higher numbers from which the median was calculated. A line between the median and low forecast would be a more accurate representation of how a majority of the panel members felt about the probability of the event occurring. It was the consensus of the panel that legislation of this type would not likely take place in the next 10 years. Panel members felt that other criminal issues such as gangs and drugs would be getting a majority of the legislatures attention in the next 5 years. However, the panel also believed that if high-technology industries began to take

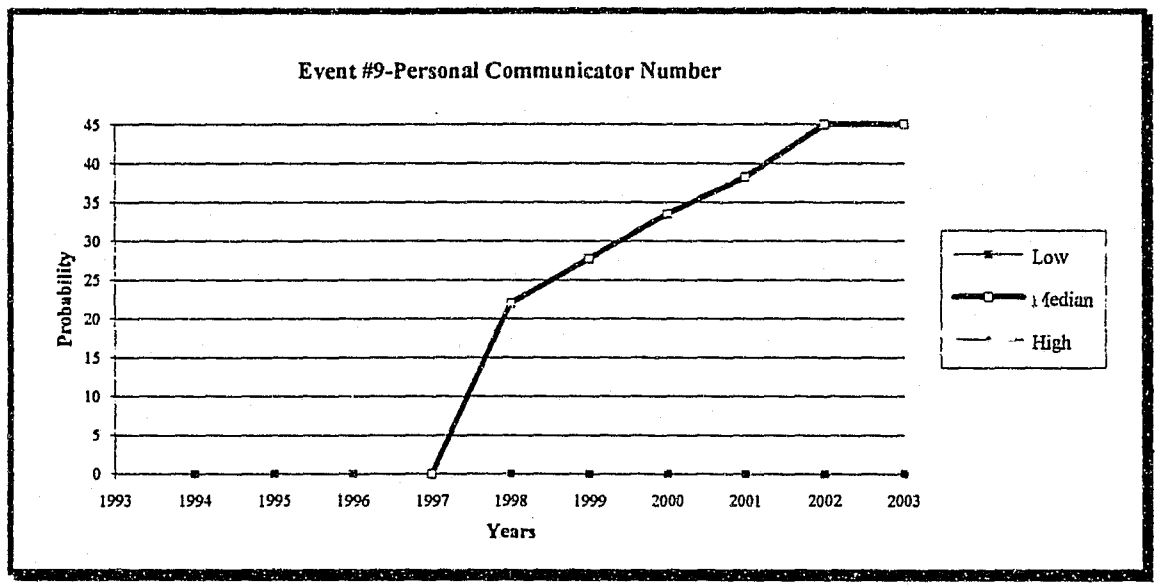
their businesses to other states due to high-technology crime issues the legislature would be quicker to act.

Illustration #19



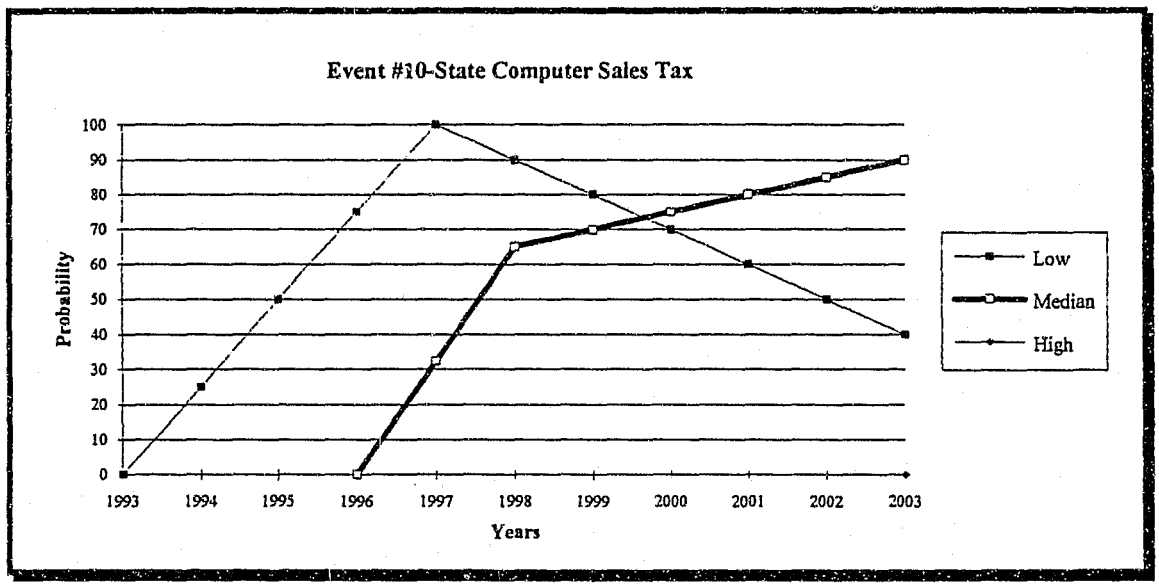
Event 8 **Private Funding:** The probability of a high-technology business providing grants to law enforcement agencies for training in high-technology crime investigation will increase towards to end of the 10th year. The graph is skewed in that the high forecast of the first year of occurrence happens in the 10th year. The consensus felt that the event would first take place in the 5th year and had a reasonable chance of occurring. Again, information relating to the high forecast graph did not appear due to the event first occurring after the 10th year.

Illustration #20



Event 9 **Personal Communicator Number:** Almost half of panel members felt the personal communicator number would not happen within the next 10 years. The high forecast information does not appear in the graph because three of the 10 of the panel members reported the event occurring 20 to 50 years from today's date. The median graph was slightly skewed upward regarding the probability of the event occurring due the high forecast data. The panel felt that there would be a relatively lower than average probability of the event occurring within the next 10 years.

ILLUSTRATION #21



Event 10 **State Computer Sales Tax:** The graph indicates that a high probability exists for the passage of a state tax on the sales of computer equipment to fund training for law enforcement in the field of high-technology crime. Discussion focused on the fact that most law enforcement resources were currently earmarked for gangs and narcotics enforcement. Very little if any funding was available for high-technology research, investigation, resources and training. The panel's beliefs may have been somewhat affected by the fact that the NGTP was conducted during the time when local and state law enforcement budgets were being significantly reduced. The panel felt that there was a very high probability of the event occurring from the five year to 10 year mark. The median for the high forecast was 90 percent. This was based on their strong opinion that an earmarked alternative source of funding was necessary for high-

technology crime investigation. Again, information relating to the high forecast graph did not appear due to the event first occurring after the 10th year.

Cross-Impact Analysis

Cross-Impact analysis is used as an instrument to assess the impact of how one forecasted event, if it occurred, would affect the probabilities of the other events.

A nominal rating scale from -10 to +10 was utilized by a cross-impact evaluation panel, three computer-related crime experts from the public sector, to assign an impact level for each of the 10 events used for this study. The event's level impact was then applied to the median probability values that were determined by the Nominal Group Technique Panel. The Initial Probabilities, median probability values, were next subjected to a mathematical formula which incorporated the cross-impact values determined by the cross-impact evaluation panel. A computerized version of the cross-impact analysis, X-mpact, was used to calculate the final probabilities of each impacted event. The analysis provided information that helped determine which events were "actor" events or "reactor" events. "Actor" events are defined as those events having the greatest impact on other events. "Reactor" events are events that are most impacted by other events. Those events where the impacts are considered near equal are "actor" events. The analysis of the impact of one "actor" event on another can be used to design programs or policies that will either enhance or reduce the probability of the event occurring. **See Table 3**

Table 3

Cross- Impact Analysis

* Level of Impact (-10 to +10 scale) Projected Over The Next 10 Years

* Initial Probability		E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	*Final Probability	
E1	70	**X**	-10	5	0	-10	0	-3	-7	0	-3	**E1**	42
E2	57	-5	**X**	10	3	2	7	2	3	0	4	**E2**	83
E3	69	-10	9	**X**	0	0	3	4	7	0	9	**E3**	91
E4	72	-8	-5	-10	**X**	0	-7	7	-6	0	8	**E4**	51
E5	69	-10	-10	0	0	**X**	0	0	0	-4	0	**E5**	42
E6	64	-10	-10	3	-9	0	**X**	0	2	-4	0	**E6**	36
E7	79	-10	-5	2	5	3	0	**X**	0	0	5	**E7**	79
E8	76	-10	10	5	4	3	2	5	**X**	0	-9	**E8**	86
E9	48	0	0	0	0	-5	0	0	0	**X**	0	**E9**	43
E10	82	-10	5	3	4	0	0	0	-10	0	**X**	**E10**	74

* Panel Medians N=12

Event Legend

Event 1	Investigation of High-technology Crime
Event 2	Major High-Technology Crime Committed
Event 3	Law Enforcement Partnerships
Event 4	Terrorist Attacks
Event 5	Smart Cards
Event 6	Entry Level Skills
Event 7	New Legislation
Event 8	Private Funding
Event 9	Personal Communicator Number
Event 10	State Computer Tax

Scenarios

Scenario writing is used to assist the researcher in clarifying the causes and consequences that trends and events would have on the policies and strategies developed for this project. It also facilitates the identification and evaluation of those policies and strategies by the researcher.

Three scenarios were developed for this project which considered which social, technological, economic, environmental, and political shifts would impact medium-size law enforcement agencies by the year 2003 regarding high-technology crime investigation. The scenarios were computer generated with the assistance of a software program provided by the Policy Analysis Company in Washington, DC . Forecasting information derived from the NGTP and cross impact review panel were utilized in the scenario generation. Seventy separate scenarios were generated and collated into three different event families. The three event families include:

1. The most likely future
2. The most desired future
3. The most feared future

Most Likely Scenario

It was initially predicted, by economists, that the recession in California would end by 1997. They also predicted that the state would experience slow economic growth for the next several years which would lead to a revitalized economy.

It's 1999 and California is still suffering from the recession of the early 90's. Economists blamed the state's sluggish recovery on illegal immigration which has negatively impacted welfare, education and other social services programs. They also state that the significant increase in the birth rates of recent immigrants has also delayed California's economic recovery.

Several high-technology and financial institutions have moved to other states which offered better tax and workers compensation incentives than California. But, the bulk of financial and high-technology companies have remained in California and have adjusted to these tough economic times.

Local law enforcement agencies, especially the medium-size agencies, have recently been experiencing an increase in the number of high-technology crime being reported (T-7). Many small retail establishments have experienced an increase in electronic fund transfer fraud and computer generated counterfeit currency, money orders and travelers checks. This increase in high-technology crime became more apparent shortly after China took over Hong Kong in 1997. This was probably due to the Asian organized crime families, Asian Triads, establishing a foot hold on the West coast high-technology markets (T-3).

A recent downward economic trend has had a significant negative impact on the investigative units of several medium-size law enforcement agencies. For the past ten years most medium-size law enforcement agencies have had to downsize or eliminate units dedicated to property crime investigation. Many of these agencies reassigned investigative personnel to patrol operations and narcotic/gang enforcement units.

Property crime investigations (includes high-technology crimes) were only worked when time permitted or if a certain monetary criteria was met (T-4).

Police managers and investigators knew they needed help in investigating crimes of this nature. At a regional investigators meeting held at the West Sacramento Police Department the topic of high-technology crime investigation was discussed. Law enforcement agencies from Davis, Woodland, Roseville, Dixon, Vacaville, Lodi, Lincoln and West Sacramento all felt that they lacked both the resources and expertise to properly investigate high-technology crime. But on the other hand, each agency was facing an increase in the number of high-technology crimes being reported and they had to find some type of solution.

A representative from the West Sacramento Police Department suggested three approaches in the investigation of high-technology crime. The first approach was to create a high-technology crime investigative task force staffed by shared resources from each participating agency. The task force concept would be the same type that was used for joint narcotic and gang units. It was also suggested that some non traditional resources, such as private industry and the local college's computer sciences department, be approached and asked if they wanted to be part of the task force. These non traditional resources could provide law enforcement with the technical, educational and computer equipment support that its desperately needs. Another non-traditional resource that was discussed but not implement at the time was the use of computer "hackers" in investigating high-technology crime (T-6). Many investigators felt that the computer

"hackers" could be used as a paid informants or "consultants" in these types of investigations.

The second approach was to investigate high-technology crimes with an emphasis on traditional investigative techniques and a de-emphasis on the use of high-technology to solve these types of crimes. It has been suggested that traditional investigative methods may be just as effective in apprehending the criminal as using high-technology specialists. Investigators felt that they could use investigative interview techniques and informants to solve most high-technology crimes. They also felt some of the traditional evidence collection techniques were skill applicable such as fingerprints but additional computer forensic training would be helpful.

The third approach incorporates both the first and second approaches into one, Cyber-Cop. Cyber-Cops are a group of specialists that are pulled together to investigate high-technology crime. The composition of the Cyber-Cop team varies from case to case. A case involving a mainframe computer and network would require a criminal investigator, computer forensic specialist, mainframe specialist and a network specialist. Another case involving Apple computers would require a criminal investigator, computer engineer, Apple computer specialist and a computer forensic specialist. Specialists with different expertise are required because the field is too complex for only one individual to know everything (T-5).

It was decided by the group to form teams (comprised of member agencies) to investigate high-technology crimes using traditional investigative techniques with the goal of moving towards the Cyber-Cop concept. The group felt that it would initially

take too long to find suitable computer specialists when there were a lot of cases that needed immediate investigation.

The topic of funding was also discussed at the meeting. A sergeant from the Roseville Police Department suggested that group solicit grants or funding from local high-technology firms.(E-8) He felt that some of these local companies may donate either equipment or money that was earmarked for high-technology crime investigation. The sergeant added that several firms provided colleges and universities with endowments for research in various area so why not law enforcement.

In Southern California, the Commission on Peace Officer Standards and Training (POST) was conducting a study discussing the necessity of providing high-technology crime investigation training in the basic academy curriculum (E-6). Renewed interest in this area was sparked by Chiefs and Sheriffs complaining to the Commission about the lack of training in this area. Several law administrators at the meeting felt that high-technology crime investigation methods belonged in an advanced officer course and not the basic academy level. They felt that the subject matter was too complex to teach at the academy level and that recruits needed to focus on firearms training and laws of arrest. Others at the meeting argued that in the near future all property crimes will be computer-related in some way. They also felt that the basic academy was a good place to start officers thinking about high-technology crime and other future issues for law enforcement. POST at this time is still studying the matter and will have a decision of whether high-technology crime investigation will be taught in the basic academy by next June.

Bank of America in conjunction with AT&T have issued the first "Smart Card" in California. The "Smart Card" was designed to eliminate the need of carrying individual credit cards for different retail establishments. It also incorporates medical insurance and telecommunication information history. The "Smart Card" also employs the latest analog encryption methods whose codes are believed to be unbreakable (E-5). The advent of the "Smart Card" could be a blessing to law enforcement in that electronic fund transfer fraud could be a thing of the past.

The California legislature has been considering a tax incentive for high-technology corporations which would provide tax rebates for those companies which provide human resources and equipment to aid law enforcement in the investigation of high-technology crime (E-10). This legislation is being opposed by the firearms and munitions lobby which believes that the same incentive should be provided to companies that provide law enforcement with specialized ammunition and ballistic characteristic information.

It should be interesting to note that a computer crime series involving electronic credit card fraud was adverted in Northern California due to the law enforcement network that was established at the regional law enforcement investigators regional meeting held at the West Sacramento Police Department in the fall of 1999.

The Most Desired Future

The great recession of the early 1990's in California had come to an end. The recession had impacted California like on other recession in the state's history. The cold

war between the Soviet Socialist Republic and the United States of America has come to an end. The defense industry in this country has begun the process of down sizing its military operations and retooling its factories for civilian application of its military technologies. This transfer of technology, much of it recently declassified, has opened new horizons for the civilian consumer market. Never before has the country experienced such a rapid evolution in the field of high-technology advances (T-9).

In addition military bases such as Mather Air Force Base, Fort Ord, George Air Force Base, Presido, and Mare Island have been civilianized and have revitalized several local economies. An example of this revitalization was the conversion of the Sacramento Army Depot into a high-technology industrial complex which manufactures and assembles computers.

Recent changes in the Federal Government's immigration policies have stemmed the growing tide of illegal immigration across California's borders. This has had a significant impact on the state's welfare and education budgets. The reduction of illegal immigration has saved California literally billions of tax dollars annually. This tax dollar savings has been pumped into programs designed to revitalize the state's business economy and law enforcement.

An innovative funding concept has also been developed by the legislature and representatives from both cities and counties to fund law enforcement and training. An enterprise fund has been developed for law enforcement which should provide a higher degree of stabilized budgets in the future. Similar to "water funds," the law enforcement

enterprise funds will be an ongoing source of funding which has been less volatile than typical general funding sources.

In the past six months Bank of America in conjunction with AT&T began issuing the first generation of "Smart Cards" to its customers (E-5). These "Smart Cards" were designed with the intention of replacing all credit, identification and phone cards with one single card. Law enforcement professionals were involved in the development process of the "Smart Cards" with the hope of reducing the numbers of victims of electronic fund transfer fraud. Others felt that that the long term applications of the "Smart Card" could be a blessing for law enforcement. Many envisioned this as a possible solution to reduce or end armed robberies and narcotic sales, especially if the card eventually replaced cash.

It has been long speculated by many law enforcement investigators that financial institutions were reluctant to report crimes such as electronic fund transfer fraud and other high-technology crimes to the local police. The financial institutions feared that the public would lose confidence in the company and bank with the competition (T-4). Financial institutions were not the only victims of high-technology crime. Local law enforcement agencies reported that there was a growing number of small retailers that were also being victimized by high-technology thieves. Almost every retail outlet used a computer for credit card and check transactions. High-technology thieves were using counterfeit checks and credit cards to bilk small retailers for thousands of dollars (T-7).

Rapid advancements in technology have created new crimes for law enforcement to investigate. Police chiefs and sheriffs complained to their legislators that the current

laws regarding high-technology crimes were inadequate and needed to updated. Prosecutors also complained about the difficulty of convicting some one for a high-technology crime because many of the rules of evidence need to be updated as well. In addition, lobbyists for several consumer groups echoed concern about computerized confidential information being stolen and then sold to third parties. They cited the example of stolen hospital medical information being used by an insurance company to deny the sale of insurance to several individuals (T-10). The Governor has convened a special committee comprised of representatives from law enforcement, the private sector, judicial and consumer groups to recommend changes or new laws dealing with high-technology crime (E-7). The Governor is also concerned about businesses leaving the state because of losses caused by high-technology crime.

High-technology companies are again one of the most rapidly developing industry in California second only to agriculture. With this renewed growth of high-technology companies and the state's economy high-technology crime also has taken off to new heights.

At a recent High-technology Crime Investigators National Conference in South Lake Tahoe California a round table discussion was held discussing how high-technology crimes were being investigated within their respective jurisdictions and companies (T-2). Attending the conference were members from both the public and private sectors who were responsible for investigating high-technology crimes within their respective jurisdictions and companies. The public sector investigators attending the conference were frustrated by the fact that most dministrations do not believe that their jurisdictions

have a significant problem with high-technology crime. A majority of those investigators felt that the private sector was hesitant in reporting high-technology crime to law enforcement (T-4). Theodore Smith, a corporate high-technology crime investigator, advised the group that there is a definite degree of under reporting being done by the private sector regarding the level of high-technology crime that is occurring. Smith advised the group that the both state and federal laws require financial institutions to reports thefts of funds, which accounts for some of the high-technology crimes (electronic fund transfer fraud) reported to law enforcement. Smith added that other high-technology crimes such as a "hacker" breaking into their computer system may be written off as a programming error or just a system malfunction.

The group also felt that there were more local businesses were being victimized by high-technology crime than people realized or imagined (T-7). Special Agent Robert Simmons with the Department of Justice offered an explanation why it was difficult to know how many high-technology crimes were being committed annually. Simmons advised the group that the current state laws do not necessarily differentiate between a high-technology crime verses a low technology crime such as counterfeiting. "Counterfeiting can be both a high-technology or low technology crime" said Simmons. In the past, counterfeiters had to have engraving and printing skills to counterfeit money. Today, many counterfeiters use computers with desktop publishing programs and color laser printers to counterfeit money. However, both crimes are classified the same with no indicator if it was a high or low technology crime. Small businesses have always been victims of check forgery, non-sufficient fund checks, and credit card fraud. "The only

difference now is high-technology is being used more and more to commit those crimes", concluded Simmons.

Representatives from both the public and private sectors also expressed frustration over boundary and jurisdictional issues regarding high-technology crime. High-technology crimes such as child pornography are committed with computers using networks such as the Internet or electronic bulletin boards to transmit the illegal images. The computer source of the material may have originated outside of the county and taken only a few millionths of a second to transmit. It appears that many different organizations, FBI to local agencies, may have concurrent jurisdiction over the same case (T-8).

The group suggested that partnerships among medium-size law enforcement agencies should be developed in combating the growing menace of high-technology crime (E-3). Conference attendees also discussed the need for a paradigm shift in how law enforcement viewed traditional jurisdictional boundary issues. Representatives from both the public and private sectors also expressed frustration over boundary and jurisdictional issues regarding high-technology crime. High-technology crimes such as child pornography are committed with computers using networks such as the Internet or electronic bulletin boards to transmit the illegal images. It appears that several different law enforcement organizations, FBI to local agencies, may have concurrent jurisdiction over the same case. The neuro-network of high speed computers has shattered traditional boundary concepts by making it possible to commit high-technology crimes from hundreds if not thousands of miles away (T-8). Private corporate security managers

attending the conference also suggested the need for the private and public sector to work together as teams in the high-technology crime investigative area. The team approach could utilize specialists in the private sector who have expertise in everything from personal computers to mainframe operations. It was also stated that it was impossible for any one individual to understand the complexities of these many diverse computer systems and applications. Attendees acknowledged that a team approach to this problem seemed to be the most plausible approach. This team approach, or Cyber-Cop concept, was currently being tested by Scotland Yard and was experiencing great success. All parties agreed to further develop the Cyber-Cop concept in their individual departments or companies and meet again in several months for additional discussions. A representative from the West Sacramento Police Department volunteered to host a meeting and take the lead in helping to develop strategies for the Cyber-Cop concept.

Representatives from both the private and public sectors also discussed various strategies of how to raise revenue for a Cyber-Cop approach to the problem. Security managers suggested that some type of tax incentive or rebate to fund the technology specialists that would liaison with law enforcement would help both the small and large businesses commit to the program. Law enforcement members also felt that this incentive or rebate program would greatly enhance their ability to properly investigate high-technology crime utilizing the right people and equipment to get the job done. A special sub-committee was formed to further investigate the feasibility of working with the legislature to develop legislation for such a program (E-10).

Attendees of the conference received some good news at the conference from a representative from the Commission for Peace Officer Standards and Training (POST). POST advised the conference attendees that it has been developing a curriculum on computer crime to be taught as a module at the Basic Academy. The representative advised that POST has been working with the University of California at Riverside for the past several years in developing an interactive virtual reality computer program which instructs students in basic concepts of high-technology crime investigation.

Approximately nine months after the conference, a series of electronic fund transfer frauds took place a various supermarkets in the Northern California area using stolen electronic security numbers (ESN) from bank cards (E-2). Computer hackers had tapped into the involved supermarkets data lines and copied the ESN information for the cards. The ESN information was then sold to an organized crime family who had a source for counterfeit bank cards. Local law enforcement agencies were quick to respond primarily due to the recently established networks and partnerships that were established after the conference. A sophisticated reverse sting operation was set up by the West Sacramento and Roseville Police Departments using electronic trap equipment loaned by the Intel corporation. Several arrest were made as a result of the reverse sting operation. One investigator noted, "If it weren't for these Cyber-Cops it would have been an impossible case to solve".

The Most Feared Future

The break up of the old Soviet Union has triggered a tidal wave of economic impacts whose aftershocks are being felt at the national, state and local levels. The President and the Congress of this country have decided to reduce the national deficit by cutting military spending due to the end of the cold war. California, in the mist of a recession, was impacted heavily by this decision to downsize the military and its industrial complex. Several military bases such as: Mather Air Force Base, Sacramento Army Depot, Castle Air Force Base, George Air Force Base, Fort Ord, Presido Army Command, Mare Island were closed in the last three years. Corporations in California such as General Dynamics, Aerojet, Northrop and McDonnell-Douglas have either closed or downsized which has had an adverse effect on the local economy. All of this was occurring when California was experiencing an explosion in illegal immigration, gang violence and narcotics trafficking.

The recession of the 1990's has left law enforcement at the lowest staffing levels in recent history. The law enforcement agencies that seemed to suffer the worst in this recession were those that were small and medium-sized. Several small agencies ceased to exist and the medium-sized agencies downsized to the point where they were barely functional. The larger law enforcement faired the best because they were more able to absorb the losses of law enforcement personnel due to developing numerous specialized positions in the past thirty years when economic times were better.

A majority of these investigative units concentrated their efforts on those crimes involving violence against persons. Drive-by shootings and car-jackings were becoming

an every day occurrence. Car-jackings have become so bad that federal legislation was passed making the crime a federal offense. The public has become afraid to walk outside their homes. The investigation of high-technology crime took a back seat to the investigation of these violent offenses (E-1).

One of the easiest and most effective methods of reducing an investigator's work load was to "pass-the-buck" to another law enforcement agency. Traffic units for years have been known for years to get on their on their hands and knees to find a trace of skidmark on an adjacent law enforcement agency's boundary in order to get out of taking a report. The same has held true with the investigation of high-technology crime (T-8). Some local law enforcement agencies work hard to find evidence that a high-technology crime took place over interstate lines so that it would be a federal case. Several federal agencies have established an investigative "dollar cap" so that only certain high-technology crimes would be investigated. Many high-technology crimes were reported to law enforcement but few were actually investigated. Experts in the field believe this was the primary reason why the private sector has failed to report high-technology crimes to law enforcement (T-4).

Recent intelligence information collected by the FBI indicated that the Russian Mafia was recruiting computer hackers to infiltrate California's Department of Motor Vehicles (DMV) computer system for their stolen vehicle rings. The Russian Mafia planned to use hackers to modify vehicle registration information in the computer system to benefit its stolen car rings (T-6). Informants advised the FBI that the Russian Mafia believed that the DMV's computer system was particularly vulnerable to this type of

attack. This was primarily due to a recent newspaper article describing the systems weaknesses and poor design.

For the past several years, foreign interests have lobbied the legislature to pass a tax on the computer industry to help fund the investigation of high-technology crime (E-7). The real reason why it wanted the tax passed was to get an advantage over its domestic competition. The legislatures attempt to get the tax passed failed. Much to the surprise of the foreign interests, law enforcement spoke out against the computer tax. At public hearings it denounced the proposed tax plan as an attempt by outsiders to rid California of its home grown high-technology industries. Little did law enforcement know at the time, it had earned an enemy for life.

The year 2002 "Smart Cards" were making their appearance for the first time in California (E-5). Touted as the ultimate secure card, it was suppose to put an end to electronic fund transfer fraud and high-technology counterfeiting. Three months after the "Smart Cards" were introduced the encryption codes were broken by a hacker employed by the Asian Triad Family operating out of Thailand. Electronic fund transfer fraud was now more prevalent than ever before. Law enforcement was falling farther and farther behind the technology curve and the criminals were gaining the superior upper hand.

In the past year the Commission for Peace Officer Standards and Training required Basic Academies to provide basic computer training to all recruits. Some law enforcement officials hailed this as a big leap forwards. Officials felt that law enforcement was preparing the next generation of officers to meet future challenges in

technology. Others chimed in under their breaths, " If they only did this five years earlier" (E-6).

Policy Considerations

What was gained by studying the future and writing scenarios depicting the most likely, most desired and most feared futures? It was a great opportunity to simulate several what-if scenarios. The what-if scenarios are powerful tools in helping shape policy considerations, planning, strategies, timing and cost benefit analysis. Policy or decision makers can use these various demonstration scenarios as clay models. These models can be shaped or manipulated to bring about the desired result or prevent the most feared future. The most desired future was selected by this researcher for the purpose of developing strategies to bring about this desired future. In addition, the desired future scenario will be used to develop policies that will help influence the desired result.

Policy considerations include:

1. An accurate assessment of businesses willing to participate in an investigative partnership relationship with law enforcement.
2. A comprehensive and complete analysis needs to be conducted on the organization's capabilities and competencies.
3. An in depth assessment of innovative and viable methods to fund the program needs to be developed by the organization.
4. City government should consider developing policy considerations that would encourage high-technology businesses to locate in the community. This could

benefit the future tax base of the city and the organization ability to gain additional resource for the high-technology crime investigation program.

5. Work within the City's political environment to gain support for the program from both a budget and master plan perspective.
6. Consider hiring non-sworn computer specialist personnel to develop and administer this type of program.
7. A volunteer or technical reserve police officer program targeting persons with high-technology computer skills should be considered for lowering the cost of staffing the program. This would also allow the department to tap into resources which it might not be able to afford otherwise.
8. The organization should conduct on going assessments of developing technologies should part be of the department's high-technology crime investigation program. Problems for law enforcement such as, encryption used by criminals, can be solved by new code breaking software programs of tomorrow.
9. Colleges and Universities with computer sciences and engineering departments need to be encouraged to be a partner in the training/research component of the organization's program. Cooperation in designing and developing a forensic high-technology criminalist course or certification program could benefit both organizations.
10. The department's micro mission statement should be developed by both the internal and external stakeholders.

SECTION III: STRATEGIC MANAGEMENT

Strategic Plan

The strategic planning process used in this study involves the development of several critical planning activities. These critical activities include development of a mission statement, conducting a situational and stakeholder analysis, identify alternative strategies and developing an implementation plan. It should also be noted that strategic planning is problem prevention. It is a systematic way to manage change and create a desirable future for the organization. The strategic plan for this study is based on the scenario which depicts the most desired future. The most desired future scenario portrays the major theme of partnerships among law enforcement agencies, the educational community and the private sector in properly investigating high-technology crime.

There are several strategic planning questions that will be addressed in this section. These include: Why do it? What is the desired outcome? What will the process look like? Who's going to be involved? What resources will it take? What will be the time frame? Strategic planning allows managers to identify and effectively manage the political aspects of the project.

The end result of the strategic planning process is the development of a structured methodology of bringing anticipation's of unknown future environments to bear on today's decisions. The desired outcomes used in this strategic planning section will hopefully assist decision makers in making quality decisions. The West Sacramento

Police Department will be used as a model to facilitate the development of these planning concepts.

Strategic Development Model

The West Sacramento Police Department was selected as a model for strategic plan development. The West Sacramento Police Department was founded on July 1, 1987 approximately six months after the city was formed. Prior to incorporation, West Sacramento comprised of four separate communities, Bryte, Broderick, West Sacramento and Southport. The City of West Sacramento utilizes a city manager-council form of government. The City is approximately 24 square miles in size and has a population of 29,000 residents. West Sacramento is located in Yolo County and its east border is adjacent to the Sacramento River. West Sacramento has one of California's two inland international deep water ports. Previous law enforcement services were provided by the sheriff's department and highway patrol. The West Sacramento Police Department employees 56 officers and 18 civilians. The Department is divided into three separate divisions: Administration, Operations and Services. The West Sacramento Police Department operates from the traditional police model of patrol being the heart of the operation. The other divisions and services are intended to support the patrol operation. The Department's operating budget for fiscal 94/95 was $5.8 million dollars.

Future-State of the West Sacramento Police Department

The West Sacramento Police Department continues to develop its expertise and pioneering approaches in combating the growing menace of high-technology crime. In the early 1990's the department began exploring the need to train its officers in the basic fundamentals of high-technology crime investigation. Subject matter experts in the field of high-technology crime investigations were brought in from both the public and private sectors to train officers in the department. Other personnel from allied agencies were encouraged to attend the training sessions.

The West Sacramento Police Department was one of the first law enforcement agencies in the area to establish partnerships with local colleges and university and formed a group of high-technology investigative specialists to assist with the investigation of these types of crimes. Several local high-technology companies in the area also offered their assistance in providing support to the West Sacramento Police Department's effort.

Investigators and crime scene identification specialist were sent to several training courses regarding high-technology crime investigation. The department was also able to obtain POST funding to send these individuals to various police and sheriff's departments in the state who have established high-technology crime investigative units. These individuals received a significant amount of on the job training from these various departments.

For the past four years the department has worked with other law enforcement and private sector agencies in developing a "team" approach in investigating high-

technology crime. A significant amount of trust and mutual respect has also developed during this time with the individuals involved.

Field officers in the past two years have been seizing more computers in vice and narcotic search warrants than before. One of the investigators stated, "I'm sure glad that we provided our officers with some training about what to and not to do when seizing computers for evidence. We have been fortunate not to have lost any information from a hard disk even when the bad guys have sabotaged the computer." Officers, investigators and identification technicians in the department are confident that they are properly investigating this type of crime and know when to call for help.

The department has implemented a recent advanced training program that will give its personnel even more tools to combat high-technology crimes in the future. This program has developed support from the local business community and the city council.

Mission Statement

The West Sacramento Police Department's primary mission is to enforce the laws of the state and city in a fair and equitable manner. The spirit of this mission is to provide a safe environment for the citizens to live in and to improve the quality of life for the community we serve.

The West Sacramento Police Department is committed to providing the highest levels of service to the community to the best of its ability. The department plans to use

both "true and tried" methods of criminal investigations as well as using advances in computer technology and science to accomplish this mission.

Micro-Mission Statement

In order to meet this new challenge of the 90's the department has established the following micro mission statement as a guide to accomplish this focused mission. This micro mission statement will assist officers in the department to better understand the department's commitment to investigate both the low technology as well as the high-technology crime.

- Management will provide support and direction in developing organizational expertise in the high-technology crime arena.
- Develop additional training programs in computer technology that will be provided to all members of the department.
- The department is committed to properly manage and investigate high-technology crimes committed in the city.
- Investigators will take innovative and creative approaches in investigating this type of crime.
- Develop effective partnerships with other law enforcement agencies and the private sector to improve solvability of high-technology crime.

- Develop high-technology crime prevention programs that will assist the business community with information about measures that can be taken to prevent this type of crime.
- Individual investigators will be given expanded authority to pursue leads regarding high-technology crime. Personal initiative will be encouraged by supervisory personnel.
- The department will improve private business sectors confidence in its ability to properly investigate high-technology crime.
- Work with the Chamber of Commerce to communicate our commitment to the business community.

Situational Analysis

An in depth analysis of the current situation regarding how will medium-size law enforcement's investigate high-technology crime by the year 2003 must be conducted in order to develop a strategic plan for the future. A process called a WOTS-UP analysis (weakness, opportunities, threats, strengths underlying planning) was used to structure the evaluation of the issue. Another model STEEP (social, technological, economic, environment and political) was incorporated to categorize the external and internal factors.

The accumulation of information presented in this analysis will contribute to the formulation, development and implementation of a strategic plan.

WOTS-UP ANALYSIS

Environment

External Threats

It appears that society's dependence on the use of computer applications is increasing at a very rapid rate. People are becoming more dependent on computers in their day-to-day life. Computers are used by many persons at their offices and homes. Students at the elementary school level are using computers in the classrooms. Businesses are becoming more dependent on computers for running everything from cash registers to check cashing verifiers. This increased use and dependence of computers by society will create more criminal opportunities in the area of high-technology crime.

Traditionally, high-technology or computer crime is looked upon by society and law enforcement agencies as being a white collar crime. White collar crime is viewed by a large segment of society as not being as important as crimes associated with violence. The white collar crimes are also treated by many law enforcement agencies as less important because the suspects are not the drug pusher types of society.

The public believes that law enforcement can cope with high-technology crime as it has done in the past with other crimes that have affected the community. Society is not aware that high-technology crime is costing corporations, financial institutions and government billions of dollars a year in losses. This losses are usually passed on to consumers in higher costs or failing businesses.

Additionally, current federal and state laws are for the most part inadequate to deal with the sophistication and complexity of high-technology crime. This hinders law enforcement's ability to properly investigate and convict criminals in this area. High-technology crime crosses local, state, federal and international boundaries. People from many different jurisdictions are affected by this type of crime.

High-technology crime, in many instances, appears to be beyond the comprehension of many citizens in this country. People have a difficult time understanding the technology that programs their VCR's without thinking about how a computer virus can destroy an entire military, governmental, or business/industry data base.

External Opportunities

There has been a growing awareness of high-technology crime, by the public, in the past several years. This was especially so in the area of electronic fund transfer fraud on the fraudulent use of credit cards. It also appears that people are paying more attention to the use of personal identification number (PIN) codes when making credit card phone calls and using bank automatic teller machine (ATM) cards for transactions.

The news media has also increased their coverage of high-technology crime in the past several years. Recent articles in newspapers and weekly magazines have featured reports dealing with breeches in telecommunication and data base security. The public has become more aware of their vulnerability to these types of crimes.

Technology

External Threats

The accelerated pace of technological innovations has opened new and more sophisticated opportunities for the criminal element to take advantage of those technologies. It appears that advances in technology are closing the door on low technology approaches to certain crimes. This will force criminals to become more sophisticated in their approach to crimes in the future. High-technology companies are reluctant to report high-technology crimes to law enforcement. Those companies believe that law enforcement does not have the ability to properly investigate crimes of this level of sophistication.

Organized crime's involvement in high-technology crime will continue to rise in the future. Organized crime has been involved in the theft of computer chips on a local, state, federal and international level. The international pirating of hardware has increased significantly over the past five years. The illegal manufacturing of computer items such as: micro processor chips, computer memory chips and peripheral equipment has taken place on an international level.

There are growing numbers of computer viruses that have infected both the micro computer and the mainframe systems. These viruses are becoming more difficult to detect and cure.

Computer software piracy has continued to grow at an alarming rate in recent years. Computer hackers are continuing to infiltrate secure computer systems such as the

Internet and Pentagon computers that were thought secure before these break ins. As more people become computer literate more hackers will emerge. Criminals are using computer modems to recruit others to commit crimes. Criminals will also use computers with encryption systems that will lock out or erase evidence sought by law enforcement.

External Opportunities

New technologies such as LOJAC (vehicle tracking device), are coming on line that can detect the location of stolen vehicles within defined geographical boundaries. The use of global position satellites will expand the capabilities of systems similar to LOJAC in the near future. In addition, new technologies will aid law enforcement in better controlling the intoxicated driver. New computerized alcohol sensing systems will be able to lock out the vehicle's ignition system if it detects that the driver has been drinking.

The expansion of computerized data bases will provide law enforcement with more criminal investigative information than before . Recent advances in latent print identification, through the use of computers, have improved law enforcement abilities to clear cases that were thought to be unsolveable in the past. Also, advances in computer telecommunication technology has allowed officers to link notebook computers, by radio modem, to the host computer systems for real time investigative data information.

The use of high-technology satellite communications has enhanced training for law enforcement officers via satellite television transmissions. POST is currently using satellite down links to police departments for video training for law enforcement.

Economic

External Threats

The continuing statewide recession continues to adversely affect law enforcement's ability to combat crime in general. This particularly impacts law enforcement's efforts to fund training for the investigation of high-technology crime.

The national debt has posed an external threat to the availability of high-technology law enforcement programs at the federal level. Currently one of the few high-technology training programs in the country is taught at the FBI Academy in Virginia.

The economic restructuring of the amount of revenue that the state passes to local governments has been in a state of flux. Since most law enforcement agencies are funded through the general fund, they are at risk of losing budget dollars. Many local law enforcement agencies have already experienced a significant reduction in the level of funding available to them in the past three years. For many law enforcement agencies personnel and programs have been reduced or eliminated.

External Opportunities

Many cities in the state have explored the feasibility of establishing special assessment districts or taxes to fund future law enforcement operations. Cities have

placed these measures on the ballot with the hope that the citizens will vote for them. Success of these ballot measures have been next to nil.

Cities and police departments are actively pursuing private foundations to fund various programs for law enforcement operations. Private foundation funding can be targeted for specialized training programs such as high-technology crime investigation training.

Housing authority funding has also been pursued by law enforcement to fund operations such as community oriented policing strategies. The West Sacramento Police Department has explored the feasibility of using this resource to fund community oriented policing programs in HUD housing units.

There are still opportunities for departments to pursue both state and federal grants to provide personnel, equipment and training for various law enforcement programs. The Office of Criminal Justice and Planning still has limited funds to automate or upgrade a department's computer equipment.

Because of California's severe recession, several private high-technology companies are assisting law enforcement with hardware and technical support. This assistance gives law enforcement agencies a better ability to investigate high-technology crime at little or no additional cost.

Political

External Threats

Politicians have focused resources and energy on issues dealing primarily with gangs, violent crimes and repeat criminal offender programs. Very little has been done to counter the growing threat of high-technology crime.

Pc .itical groups such as the American Civil Liberties Union (ACLU) have lobbied the legislature to enact laws that would prohibit or limit law enforcement's ability to use certain technological advances to intercept computer or telecommunication systems used by the criminal element to commit crimes. The ACLU has argued that the right to privacy must not be violated by law enforcement. They claim that use of certain advanced technologies will violate those rights.

Many city politicians have limited knowleage of the growing problems associated with high-technology crime. Their primary concern deals with public safety. A Chief of Police would find it difficult to implement programs relating to high-technology crime in a time of increasing gang violence.

External Opportunities

The more hackers penetrate or sabotage national security data bases, legislation will be enacted to give law enforcement more latitude in investigating this type of criminal activity.

As more major corporations become high-technology crime victims due to electronic fund transfer fraud, telecommunications fraud, and stolen information from data bases, pressure will be placed on the legislature to act. It will be lobbied for more legal protection and stiffer penalties for those who break the law.

The Organization's Capabilities

The West Sacramento Police Department is typical of many medium-size law enforcement agencies in California. The Department is organized into two divisions: Operations and Services. The Operations Division consists of the patrol and investigations units. The investigations unit has responsibility for investigating any serious crime that occurs in the community. It also has responsibility for investigating those cases that a patrol officer has neither the time nor the expertise to investigate. The Services Division has responsibility for managing records, communications, data processing, training, facilitates/maintenance and internal affairs.

Internal Strengths

The department has been a recent recipient of an Office of Criminal Justice and Planning Career Criminal Apprehension Program (CCAP) grant. The CCAP grant provided resources to purchase software and hardware upgrades for the mini mainframe computer system. It has also helped the department move towards a more technologically advanced working environment.

The department has also been working to develop a data processing system plan. This plan addresses the use and types of security required for department computer operations. Recently, the department established an in-house computer user committee that will address all computer-related needs and issues in the department. This committee consists of the Services Division Lieutenant, crime analyst, records manager, a department computer expert and representatives from the city's data processing unit.

The Services Lieutenant has been a member of the High-technology Crime Investigators Association for the past several years. He has been assigned the responsibility of presenting new information as it relates to high-technology crime to both members of the user committee and investigative personnel.

There has been an increased awareness by members of the department regarding the security and confidentiality of department computers. They are also more aware of the vulnerability of the micro and mini mainframe computers to unauthorized access and sabotage.

Command staff, sergeants, officers and non sworn personnel have been pursuing city sponsored classes in word processing, data base management, spreadsheet and mini mainframe computer applications. Approximately 80-90 percent of the department use computers at this time.

City data processing recently hired a new programmer who is knowledgeable about computer security systems.

Internal Weaknesses

Level of computer literacy by most members of the department has been considered low by data processing department standards. There has been some direction given by Command staff that officers/investigators should receive additional training in the area of computer crime.

If faced with a high-technology crime series tomorrow the department would have to depend on outside agencies such as the Department of Justice or the FBI for assistance to investigate a case of this nature.

Stakeholder Analysis

The stakeholder analysis conducted looked at those individuals or groups which have an impact on what can be done or impacted by the plan that was designed. Stakeholders have a vested interest in the issue or program that may be implemented. They have a concern over any effort to change the issue. They also may have some ability of influence on the issue or program.

A *snail darter* is an unanticipated or planned stakeholder who could have a catastrophic effect on the plan or strategy that might be employed. A snail darter has the ability to make major change or stop a program.

The following list of stakeholders was developed after reviewing the WOTS-UP analysis of this paper. Stakeholders both internal and external to the organization were identified as having an impact on the strategic plan or being affected by it. They are also

individuals or organizations that would have a definite interest in any outcome, strategy or impact that this plan would produce.

Stakeholder Assumptions

1. City Council - The City Council (which includes the Mayor) will hold the following assumptions on improving police department expertise in investigating high-technology crime:
   a. Will adopt or support any effort that will keep their constituency (citizens and business community) satisfied. They will act on a political basis of getting elected and view constituency support as important to that purpose.
   b. Will adopt a position of fiscal cost effectiveness. In these days of recession and fiscal accountability the council will only support programs that demonstrate cost efficiency and effectiveness.
   c. Are very interested in innovative programs that will help develop the community into a Premier City.
   d. Will be supportive of the police department's efforts of improve the level of service to the community.
2. Chief of Police - The Chief of Police will hold the following assumptions on improving the department's ability to investigate high-technology crime.
   a. Will keep the department current with the changes in technology.

b. Will be concerned about the impacts of department reorganization and how it will affect efficiency and investigative effectiveness of future programs.

c. Will support the concept of maximizing the use of technology as a department priority.

3. Department of Justice - The Department of Justice will hold the following assumptions to better law enforcement's ability to investigate high-technology crime.

a. Will assist local agencies with high-technology criminal investigative support programs and technical expertise.

b. Will work with local law enforcement agencies to develop and provide training in this future field.

c. Will want to assist local law enforcement agencies with all types of criminal investigations especially high-technology crime.

4. High-technology Companies - The High-technology Companies will hold the following assumptions in assisting law enforcement agencies to develop improved expertise in the investigation of high-technology crime.

a. Will be concerned about the lack of expertise or training that law enforcement has in the high-technology crime area and are likely to be willing to assist them with technical expertise when requested.

b. Will work with local law enforcement agencies in an effort to have hardware and software "pirates" successfully prosecuted.

c. Will support law enforcement efforts to better investigate crimes involving the use of high-technology.

d. Will be concerned about trade secret information being compromised during criminal prosecutions.

5. Private Investigation Companies - The Private Investigation Companies will hold the following assumptions as it impacts their ability to generate revenue in cases involving high-technology crimes. *(possible snail darter)*

a. Will view high-technology crime investigation as a foreseeable large revenue source in the future.

b. Will continue to be supported by the private sector in investigating internal and external security problems that the company may be experiencing.

c. Will have access to information unavailable to law enforcement.

d. Will view increased law enforcement involvement in this area as a threat to their business (competition).

6. Commission on Peace Officers Standards and Training (POST) - POST will hold the following assumptions on improving law enforcement's knowledge and expertise in the area of high-technology crime investigation.

a. Will train officers with the latest resources available in the investigation of high-technology crime.

b. Will be futures oriented regarding changes in technology and will maximize the use of the latest technologies.

7. American Civil Liberties Union (ACLU) - The ACLU will hold the following assumptions in protecting the constitutional rights of citizens in this country.

   a. The ACLU will oppose anything, including technological advances in investigating high-technology crimes, that infringes on privacy issues brought on by advances in technology.

   b. Will be concerned with freedom of speech issues generated by telecommunications advancements and items such as the National Security Agency's Clipper chip concept.

   c. Will strongly oppose legislation that will give law enforcement access to computer hardware and software systems.

   d. Will oppose law enforcement and private sector collaboration due to privacy issues and due process.

   e. Will actively lobby to keep law enforcement restricted with respect to any type of computerized information that they have access to and how that information can be used.

8. Police Department Labor Organizations (PDLO) - The PDLO will hold the following assumptions on improving working conditions, increases in wages and benefits for its members.

   a. Will support computer training that will enhance the skills and career enhancements for department employees.

   b. Will be concerned about repetitive motion issues related to the use of computers by employees.

c. Will be concerned about the possibility of technical support persons working outside their job descriptions in the investigation of high-technology crime.

d. Will be concerned that further computerization of the department may lead to less jobs for people represented by their organization.

9. Command Staff - The Command Staff will hold the following assumptions on improving the department's ability to investigate high-technology crime as well as other organizational issues.

a. Will support the need of computer training for department personnel.

b. Will be concerned about what types and cost of training needed for high-technology crime investigation.

c. Will weigh high-technology crime investigation against other investigative needs of the organization.

d. Will view high-technology crime as not a priority for the department at this time.

e. Will be concerned that the police department may never be able to develop the in-house expertise to investigate high-technology crime. Willing to explore the use of consultants or civilian experts in this field.

10. Chamber of Commerce - The Chamber of Commerce will hold the following assumptions to improve conditions for businesses in the community.

a. Will support the concept of the department developing a high-technology crime investigative component as an incentive in attracting new business to the community.

b. Will support the development of partnerships with law enforcement and the business community to fight high-technology crime.

c. Will be concerned that high-technology crime investigation is not a priority for small businesses in the community.

11. District Attorney - The District Attorney will hold the following assumptions to improve the successful prosecution of high-technology crimes in the county.

a. Will support the need for a high-technology crime investigation unit in the department.

b. Will be concerned that resources will not be available to support activities in high-technology area; resources placed in crimes of violence.

c. Will be concerned about lack of in house expertise to successfully prosecute high-technology crime cases.

12. Police officers - The Police Officers will hold the following assumptions to improve their ability to properly investigated high-technology crimes. Also to improve their skills, knowledge and abilities in an area that may help in their future promotablity.

a. Will support the need for additional training in the area of high-technology crime.

b. Will have a strong interest in improving computer skills and knowledge.

c. Will still be intimidated by computers but to a lesser degree.

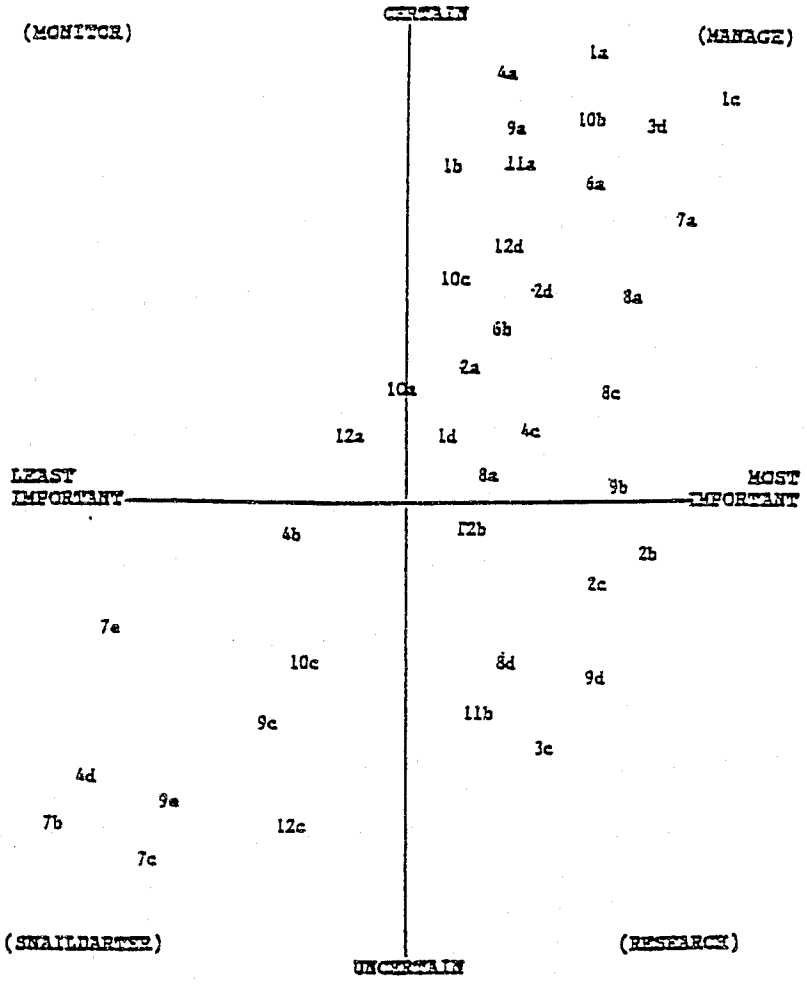
d. Will support the use of computers to help them solve crimes faster and more efficiently.

Stakeholder Assumption Mapping

For an illustration of the individual assumption positions, the forecast certainty of each assumption, and the level of their important are located on the Stakeholder Assumption map. The mapping of the various assumptions assists the researcher in identifying and considering those assumptions which may be critical to the strategic plan.

Illustration #22

Stakeholder Assumption Mapping



Stakeholder Legend

1. City Council
2. Chief of Police
3. Department of Justice
4. High-technology Companies
5. Private Investigation Companies
6. POST
7. American Civil Liberties Union
8. Police Department Labor Groups
9. Command Staff
10. Chamber of Commerce
11. District Attorney
12. Police Officers

Developing Alternative Strategies

Three strategies were selected for this project by using a modified policy Delphi process and discussion. The panel consisted of a Deputy Chief from a large size department; a Lieutenant from of medium-size law enforcement agency; a Captain from a medium-size law enforcement agency and a Lieutenant from a large size law enforcement agency. The panel discussed each of these strategies in detail. They were instructed to give careful consideration to the advantages and disadvantages of each unique strategy. The strategies vary in approach but each is relevant to the overall mission goal. The panel generated ten strategies during the first round of the modified policy Delphi process. It was during this round that several ideas generated by the panel were combined to produce a single inclusive strategy.

Recommended Alternative Strategies

1. Law enforcement should form an association with federal, state, local and private sector high-technology specialists to promote liaison, lobbying, training and legislative change in this area. This would promoted and encourage public/private sector partnerships.
2. Establish a fellowship exchange program with law enforcement and the private sector to share experiences, information and training.
3. Implement a tax on the sales of computer equipment to fund law enforcement training in the area of high-technology crime investigation.
4. Legislate law enforcement powers of arrest to private company high-technology investigators.

5. Contract with the private sector to investigate high-technology crime.

6. Investigate high-technology crimes for other law enforcement agencies and charge them for the services

7. Have the Department of Justice responsible for the investigation of all high-technology crime at occurs in the state.

8. Hire "hackers" as consultants to assist law enforcement agencies in the investigation of high-technology crime.

9. Provide a tax incentive to private high-technology companies to fund technical assistance to law enforcement in the investigation of high-technology crime.

10. Develop a "pool" of high-technology technicians that law enforcement can draw upon when needed to assist in the investigation of high-technology crime.

STRATEGY I: *Law enforcement should form an association with federal, state, local and private sector high-technology crime specialists to promote liaison, lobbying. training and legislation. This will promote and encourage public/private sector partnerships in solving high-technology crime.*

With this alternative, the West Sacramento Police Department would focus on trying to develop relationships or partnerships with these various organizations and professions. The common theme that would be used to draw these organizations together would be, "We Need Each Other's Help."

Law enforcement agencies realize they lack both the technical expertise and equipment to properly investigate this type of crime. Also, many of these agencies lack the human resources necessary to conduct these lengthy investigations. A similar strategy was used successfully in Yolo County twenty years ago to investigate arsons.

Local law enforcement and fire agencies lacked both the technical expertise and equipment to properly investigate arsons. Both federal and state resources were use to supplement resources at the local level. Expertise that the local jurisdictions lacked were later developed through training classes and on-the-job training.

This strategy would use a model similar to the arson team model that was used over twenty years ago in that county. However, one of the first things that needs to be accomplished is for people to agree that the individual jurisdiction have a problem with the investigation of high-technology crime. A sense of urgency needs to be created by the participants in this effort for the plan to be implemented by policy makers.

Positive Aspects of the Strategy

The one of the most positive aspects of this strategy is the development of the partnership concept of investigating high-technology crime between the public and private sectors. The partnership relationship is based on a mutual goal by all parties involved, to improve the quality of high-technology criminal investigations. The consistency of the investigations would also improve in this positive environment of partnerships. Law enforcement and private sector investigative personnel would be able to combine resources to defeat the common foe.

This strategy would also increase stakeholder "buy in" of mutual bilateral support. Law enforcement would have access to state-of-the-art computer technology in both software and hardware. It has been well known in educational circles for the past several years that private industry sits on the cutting edge of technology. "The

educational system, colleges and universities, can not provide law enforcement with current or breaking technological information," states Dean Susan Hackwood of the University of California at Riverside. The educational system will always be behind the private sector in research and the development of high-technology. This makes it imperative that law enforcement and the private sector work to develop long term partnerships in this area.

Most importantly this strategy would opens lines of communications between the private sector and law enforcement agencies. This will also go a long way in helping to develop mutual respect and trust for the parties involved. The personal relationships developed by this strategy can either help or hinder this program more than most people will acknowledge. In fact, success or failure of this strategy rests more with those emerging partnerships than the program itself.

Negative Aspects of the Strategy

One of the negative aspects of this strategy is the fact that it will take a lot of time to organize, plan and keep this program active. The right people need to be involved in the start up of this project if it is to get off on the right foot. The right people would be part of the critical mass and might be difficult to recruit.

This strategy may also create a new bureaucracy which could reduce the effectiveness and efficiency of the investigative partnerships. This bureaucracy would probably take away resources (money) from where it was actually needed. Regarding resources, a program such as this would probably have some high start up costs. The cost

of the computer software and hardware could be considerable. The cost of staffing would affect both public and private sector payrolls.

Another negative aspect of this strategy is a high probability that the hardware and software necessary to investigate this type of crime may not be available. The FBI acknowledges that their field offices are ill equipped to investigate complicated cases of high-technology crime. Much of their hardware and software for these case are located at FBI headquarters. Local medium-size law enforcement agencies may not have access to code-breaking or system analysis software. Much of this software may only be available at the National Security Agency level.

In addition, there are very few people qualified to train and educate law enforcement personnel in how to properly investigate high-technology crime. As stated earlier the colleges and universities currently do not offer courses in computer forensics or criminology. There are only a handful of high-technology investigated courses offered in the nation. One course has been taught in the Sacramento area, with the other investigative courses offered on the east coast.

Stakeholder's Perceptions

The strategy of forming partnerships with the public and private sectors was met with enthusiasm by most of the stakeholders. The Chief of Police and the Command Staff felt that the officers would benefit from the training and dialog that they would receive from the private sector. They are also encouraged by the possibility of improving the coordination of cases if all parties were communicating with each other. This was

particularly important because these cases were constantly crossing jurisdictional lines within a nano second (millionth of a second).

Members of the private sector would be also enthusiastic about the possibility of working with law enforcement as partners in combating growing high-technology crime problems. However, the American Civil Liberties Union (ACLU) is very skeptical about this newly formed partnership. They feel that law enforcement would have more information available to them such as spending habits, credit history, medical records that could be used to build dossiers on people illegally. They also protested the point that law enforcement would have greater access to private information, thus violating privacy laws.

Private investigation companies feel that law enforcement was infringing in an area that originally had been their turf. In the past, any private investigation firms were hired by companies, including high-technology companies, to investigate internal theft, computer fraud and internal sabotage. It is perceived that several large private investigation firms would lobby the legislature to pass laws that would limit the information that the private sector could legally release to law enforcement.

This plan is very appealing because it has a good possibility of success. Improved communications with other parties is bound to benefit everyone involved. Some of the concerns that the private investigations firms have can be mitigated by having some positive dialog with them and involving them in the planning process.

STRATEGY II: *Establish a fellowship exchange program with law enforcement and the private sector to share experiences, information and training.*

The concept of developing a fellowship exchange program with law enforcement and the private sector was met with enthusiasm by the panel. This strategy was supported by most panel members as being a method of establishing long-term relationships between the public and private sectors.

This strategy was also looked upon as an interim solution until a program such as Cyber Cop could be established. The strategy works along the theme of the private and public working together in order to solve a common problem. The strategy could involve fellowship programs that ranged from two weeks to one year in duration

Positive Aspects of the Strategy

This strategy would give law enforcement a better understanding of the high-technology business environment. Law enforcement agencies have a limited understanding of how most of these high-technology companies operate. For example, many police officers have a cursory understanding of how cellular telephone systems operate. This lack of understanding makes it more difficult for officers to investigate one of the most serious high-technology crimes occurring today, electronic phone fraud.

The private sector would also benefit from this strategy. They will gain useful insights about criminal investigations and the justice system from a law enforcement perspective. The technicians, analysts, and investigators of these private sector companies will be more able to assist law enforcement agencies with these types of high-

technology investigations in the future. They will know what it takes to build a case to get a conviction in court.

This strategy would be a low cost program to both participating parties. It will also be cost effective from a training standpoint. The panel members suggested that part of the strategy would be to develop an economic incentive (tax) to fund a program of this type in the future for private sector participants.

.Another benefit of this strategy would be law enforcement improved ability to recruit computer-literate people into the profession. This would help develop the Cyber Cop concept of having law enforcement personnel with computer investigative skills. Again, trust and improved communications will happen between the public and private sectors with this strategy.

Negative Aspects of the Strategy

One of the most negative aspects of this strategy is the fact that the fellowship program would effectively remove an officer from the department for that period of time. The same would hold true for members of the private sector. This would be especially important for organizations that are experiencing shortages in human resources during difficult budget times.

Another possible drawback to this strategy is the possibility of the law enforcement officer being recruited by the private sector to investigate high-technology crime. The prospect of making a higher salary in the private sector could leave gaps in a medium-size law enforcement agency's ability to investigate high-technology crimes in

their jurisdictions. In addition, citizens in the community may not think this is the best use of limited police resources during a time when violent crime has been on the increase.

Stakeholder's Perceptions

This strategy would receive mixed reviews by several stakeholders. Many stakeholders would feel that the concept of a fellowship was an excellent idea. It would provide law enforcement with the training that it needs at little or no cost. The City Manager's office and the Chamber of Commerce were the first to support the concept.

The Chief of Police and Command Staff felt that conceptually the idea of having a fellowship with the private sector would benefit all parties involved. This is mainly due to the fact that officers would benefit from learning more about high-technology and would be able to use the most modern and sophisticated equipment available. They soon would have second thoughts about losing an officer for a given period of time after they had time.

Times are tough and budgets are lean. The Command staff would not feel it would be able to free up one officer, given the current workload they were experiencing. This is a more difficult issue for small and medium-size law enforcement agencies due to the limited resources they have available.

Still, the concept would generate some interest among various law enforcement agencies and some private sector companies. It is suggested that the fellowship exchange program could be designed in a multitude of ways. For example, the length of time of

the fellowship program could be negotiated. In addition, an agreement could be worked out that would allow the officer to be used by the department if there was a severe need and so on.

This plan would gain the support of the department's labor unions. The labor unions have always supported the concept of job enrichment. They viewed the fellowship exchange program in a very positive manner. They feel that the program would not only help the employee learn some new job skills but provide him/her a break from the stress of police work.

Another benefit of the program that a majority of stakeholders support is the fact that the fellowship exchange program would build a positive and long lasting bond between law enforcement and the private sector.

STRATEGY III: *Implement a tax on the sales of computer equipment to fund law enforcement training in the area of high-technology crime.*

Strategy III involves the concept of instituting a sales tax on computer equipment to fund training for law enforcement in investigating high-technology crime. The panel expressed mixed feelings about the feasibility of this strategy. Initially, the panel felt that this was an excellent method of raising funds to provide training for law enforcement in the investigation of high-technology crime. In order to invoke this strategy, some organization would have to lobby the legislative and executive branches of government to pass such as tax. The only other method of instituting a tax of this type would be through ballot referendum.

During discussion of this strategy the panel discussed the possibility of instituting a tax incentive program instead of a tax on computer equipment to accomplish the same goal. It was thought that an incentive program would be seen as more positive by the business community than a tax.

Positive Aspects of the Strategy

During difficult economic times this strategy would be seen be some to be a possible source of untapped revenue. Literally millions of dollars could be generated each fiscal year that were dedicated to training law enforcement officers in the investigation of high-technology crime. Taxing business to pay for services that are generated by their operations would be considered positive by a percentage of the population.

Again, the though of this user tax would be a growing revenue source in the future. Many felt that the computer or high-technology field would continue to grow considerably in the next ten to twenty years in California. It would be a crime specific tax that taxed the very industry that was having the problem. This tax would also make it possible to fund high-technology investigative programs that could be coordinated on a state wide basis.

Negative Aspects of the Strategy

This strategy would create a schism between the private and public sectors. There would definitely be a lack of computer industry support for a tax of this type.

Instead of establishing partnerships in combating high-technology crime resistance would be created. Computer/high-technology companies may even be forced out of the state in order to remain competitive in the open market. There would also be a lack of consumer support for this strategy. The consumer in California would be paying more for the same equipment than someone else in another state.

Many citizens feel that high-technology crime is white collar crime and any funds generated should be spent on gang and narcotic enforcement.

This strategy also requires legislation or a tax initiative to be passed. There would be a remote possibility of a tax of this type reaching the governors desk for signature while California is still struggling in a recession. As stated earlier, there will be a good possibility that high-technology companies would relocate outside California with a tax of this nature.

Stakeholder's Perception

This program probably would be met with the most diverse review by the stakeholders involved in the process. On the public sector side of the equation most stakeholders feel that this strategy is an untapped resource just waiting to be used. They feel that this plan would help finance much of the needed training, equipment and research necessary to properly investigate high-technology crime.

On the other hand, stakeholders representing the private sector side of the equation feel that this would not be the best solution to the problem. Many of them acknowledge the fact that law enforcement is in need of a funding source to finance

training, equipment and research. Private sector companies and the Chamber of Commerce feel that this tax would place an undue hardship on computer companies and manufacturers in California. The private sector companies believe that the state has already makes it difficult for companies to operate in California due to its current workers compensation and tax laws. They also feel that this new tax could cause them to be not as competitive in the open market. The Chamber of Commerce felt that this innovative tax might be the straw that would break the camels back.

If this plan was implemented, careful thought, consideration and planning must take place if there would be any hope of legislation of this type being passed. Instead of working together with the private sector in a positive partnership relationship this strategy could drive the groups apart.

The Preferred Alternative Strategy

The preferred strategy for implementation of this plan is STRATEGY I. The panel feels that Strategy I would go a long way in helping medium-size law enforcement agencies investigate high-technology crime in the future.

Strategy I incorporates the most important components in the successful investigation of any crime, information and cooperation. If Strategy I is properly organized and structured, it could evolve from a local system of information exchange, training and joint investigative ventures to an association at the international level similar to INTERPOL.

Implementation Plan

In order to effectively implement any strategy or plan there needs to be a clear understanding of the basic structure of the plan by all parties involved. This structure must include definition of the goals and objectives of the plan and a course of action to accomplish these goals and objectives. There are also additional points of the plan that should be not only discussed but more importantly thoroughly understood.

These additional points include:

- Develop methods to get private sector support and buy in for the plan.
- Develop methods to get internal support and buy in for the plan.
- Investigate methods to get Council and City Manager support.
- Develop ideas of getting the various law enforcement agencies to buy into the concept.
- Develop the program in small manageable increments.
- Explore the concept of how formal or informal does the department wants to be.
- How will the department keep people interested and motivated to accomplish more?
- Develop a plan of how to get and keep the Chief's support of the project.
- Identify key individuals in both the public and private sector who will provide the foundation of the plan.

- Create a coordinating team that will do much of the initial leg work for the project.
- Develop a liaison with the local colleges (computer science departments) and see if they are interested in being part of this plan.
- Investigate the use of volunteers to help organize meetings and do some of the paper work.

The above mentioned items are some of the important things to keep in mind when trying to implement a plan. There certainly are numerous other factors that will need to be added and discussed as the plan progresses.

Phase 1

An initial requirement of this plan would be to contact various parties in the area and establish an interested parties list. There are lists published by the SEARCH group in Sacramento and the Northern California High-technology Investigators Association (HTCIA) from which interested parties can be contacted. Also, inquires should be sent to the faculties of the local universities and colleges inquiring if they are interested in being part of the plan.

Once a list of interested parties is established the Services Lieutenant would serve as the initial facilitator and coordinator for the program. People will be encouraged to discuss the topic in an open and semi-unstructured forum. At this time the facilitator should bring up the idea of formalizing the meeting as a committed event. People agree to meet again and attempt to formalize the association.

Phase 2

In phase 2 this new association will become more formalized. Initial planning concepts will be developed by members of this group. This new association will embrace the concept of the private sector working with the public sector in investigating high-technology crimes. It is different from associations in the past in that it will be openly investigating cases that effect both organizations. This phase would also formalize each agency's commitment to the plan. Members of this association should be well aware at this time that the department is committed to the investigation of high-technology crime.

Phase 2 will focus on formalizing the plan and getting people first to develop personal relationships before getting to the task of conducting organizational strategies. Personal rapport at this phase of the program is considered an important ingredient to overall success of the plan.

SECTION IV: TRANSITION MANAGEMENT

Transition Management

Situation

Computer-related crime can be defined in several different ways. Computers can be the objects of crime. Examples of this include contents of the computer damaged, blown-up by a bomb, or destroyed by a complicated computer virus. Computers can also be subjects of crime. Computers can be the environment which frauds are programmed into and the crime is carried out. Computers can also be instruments of crime. Computers have been used to plan and control criminal acts that are complex and sophisticated in nature. These crimes have included money laundering, electronic transfer fund fraud and embezzlements. The computer programmer or operator can use the computer as an instrument of the crime to steal valuable information from an employer.

Computer crime is growing at an ever increasing rate in both the state and nation. Most people associate computer crime as a crime committed by some person(s) with special knowledge of computer technology. In the past several years there have been increases in "white-collar" crime which is being associated more and more with high-technology crime. The increase of "white-collar" crime can be attributed to more business becoming automated and the fact that "information" is becoming more valuable.

These types of computer or high-technology crime were first reported to law enforcement agencies in the late 1950's. The crimes included: fraud, theft, larceny,

embezzlement, burglary, sabotage, espionage, murder and forgery. These crimes are not too dissimilar to the types of computer-related crimes that are reported today.

Most of these types of computer-related crime is committed by "trusted" computer users in the company. Many of these trusted computer users commit crimes by entering false data into the computer. They have also been involved in electronic trespassing, stealing copyrighted information, piracy and vandalism. Industry experts estimate that theft of information from computer data bases may cost the industry over 20 billion dollars a year.

Present

The West Sacramento Police Department acknowledges that it is currently ill prepared to properly investigate most types of high-technology crime. Organizationally, it has done little to prepare its officers in learning and understanding new technologies such as computers and other high-technology advances.

Many members of the department, including management staff, do not have an adequate level of comprehension regarding the complexities of computer-related high-technology crime. Some department members are somewhat intimidated by advances in computer technology. They are more at ease investigating more traditional crimes such as burglaries, robberies and homicides.

The department has made the commitment to begin training its officers in the use of computers. Currently, the department is sending personnel to computer training sponsored by the City Data Processing unit. There has been a heightened level of interest

by many members of the department to improve their knowledge about computers and their applications.

In addition, the department recently established a computer/technology committee which is comprised of members of the Police Department and Data Processing. This committee is charged with the responsibility of evaluating the department's current and future computer needs, resources and training. This committee is in the process of writing the computer plan for the department and has been a stimulus for Data Processing in developing a similar plan for the city.

Recommended Strategy

The future scenario described in the futures study component of this paper discusses the evolution of a new type of high-technology crime fighter called "CYBER-COP". Cyber-Cops will be a hybrid of a law enforcement officer with a high-technology computer background. Initially, the West Sacramento Police will develop partnerships with private sector businesses and other law enforcement agencies to solve these types of crimes.

An in-depth analysis of the current "situation" regarding this issue was conducted by this writer. A process called a WOTS-UP analysis (weaknesses, opportunities, threats, strengths, underlying planning) was used to structure the evaluation of this project. Another model, STEEP (social, technological, economic, environment, political) was incorporated in the study to give the writer a more defined scope of what external threats and opportunities may impact the project.

As the West Sacramento Police Department begins to move from its present state towards the future a transition period will take place. The change agent must help the organization focus on the importance of implementing the plan of improving the quality of criminal investigation involving high-technology crime. A vision needs to be created so that the personnel involved with the project can get a sense of where the department wants them to be in the future. Most importantly, a sense of organizational urgency needs to be created regarding the growing number of high-technology crimes that the department lacks the personnel, sophistication and proper training to properly investigate. The change agent must present people in the organization with a common vision of shared values regarding the necessity of carrying out the mission in the organization. It is also necessary to prepare members of the organization for the struggles and challenges that lay ahead for them with this project. It is also important to communicate to them that the emphasis of this project is for the long haul and that short term sacrifices may have to be made in order to be successful.

Management needs to effectively communicate to the organization and stakeholders the following:

1. Establish simple and high standards for the program.
2. Keep people in the department informed on the changes that are happening.
3. Involve department personnel in problem solving.
4. Identify the resources necessary in carrying out the mission.
5. Improved communications and education with the business community

regarding high-technology crime.

6. Management must pay attention to detail.

7. Create a spirit teamwork through strong unit identity and controlled internal competition.

8. Make sure that the right people are in the right places.

9. Create a level of dissatisfaction in the organization with the manner in which high technology crime is currently investigated.

10. Keep people constantly informed and up-to-date with the status of the project.

Critical Mass

To have a successful transition the Critical Mass must be identified. The Critical Mass is comprised of a minimum number of people who will play a major role in the success of the project. However, if they oppose the transition plan it maybe doomed to failure. In addition, the Critical Mass is made up of persons who interact with the stakeholders. The difference between being a stakeholder or critical mass member is that stakeholders are individuals who have a vested interest in the plan. Stakeholders will be affected by the results and have some impact on the plan both positive or negative. Critical Mass members are action oriented. It is comprised of people or groups who will either make the plan happen or keep it from happening.

A very important part of this transition plan is to properly identify those persons or groups who comprise of the Critical Mass. This writer, with the assistance of senior

law enforcement administrators and department middle management staff, attempted to conduct a realistic assessment of the Critical Mass' readiness for change. At least one member of the Critical Mass must be at the "make it happen stage". This individual(s) is the driving force that will pull the transition through the various peeks and valleys that will happen throughout this process.

It is also critically important to identify any individuals or groups who are in the Critical Mass that are currently in a "block change" position. These individuals or groups need to be repositioned from that position to at least the "let it happen" stage to facilitate the plans success.

To more appropriately assess the members of the Critical Mass a commitment planning chart was completed. **See Table 4**

Table 4

Critical Mass Commitment Planning Chart

LEVELS OF COMMITMENT				
Key Actors	Block Change	Let Change Happen	Help Change Happen	Make Change Happen
City Council		X		O
City Manager			X O	
Mayor	X	O		
Chamber of Commerce			X O	
Chief of Police			X	O
Police Captain		X	O	
Dept. Lieutenants		X	O	
Special Projects Lieutenant				XO
Detective Sergeant			X	O
Director of Data Processing		X	O	

Panel Medians N=3

X = Current Commitment **O = Needed Commitment**

In the City of West Sacramento the following members have been identified as the critical mass impacting the implementation of the Cyber Cop program:

1. City Council
2. City Manager
3. Mayor
4. Chamber of Commerce
5. Chief of Police
6. Police Captain
7. Department Lieutenants
8. Special Projects Lieutenant
9. Detective Sergeant
10. Director of Data Processing

City Council

The City of West Sacramento has five council members who are elected at large. The Council appoints the Mayor and Mayor Pro-Tempore by council action. Two years ago the Council adopted a mission statement for the City. The Council described several goals that the City wanted to achieve in order for it to be the Premiere City of the Sacramento region. This mission statement is very futures oriented and fits in well with the police department's high-technology crime program. Collectively, the City Council can make or break any project that the city entertains. The current position of the City

Council, collectively, is in the *let it happen* stage. There appears to be slightly more than minimal support at this time for the Department's project. None of the Council members at this time are in the "*block*" position. Several members of the Council view this project as having *shining star* potential.

Since incorporation, seven years ago, the City of West Sacramento has attempted to change its tarnished image in the region. In the past eight years the City of West Sacramento has spent millions of dollars to improve its roads, sewers and water supply systems. It has also invested millions of dollars in redevelopment projects to revitalize the community. It wants to be recognized as a city of tremendous growth and opportunity.

The City Council has been very supportive of projects that enhance the image of the community. The Council has the opportunity to be a leader in this area and encourage businesses that are either high-technology oriented or have a high victim profile for computer-related crimes to locate in West Sacramento. A strong show of commitment and support by the council is critically important for the success of this project. The most desirable level of participation of this critical mass group is to make change happen.

Several things need to happen if this critical mass group is to be moved to the make change happen stage. First, the council needs to be convinced that this program is going to be of great benefit to the city from both an economic and political point of view. The Council needs to be provided with detailed information about what the capabilities of the Police Department are in this area and what the future may behold for the city.

This information will be addressed in the five year plan. Second, realistic expectations should be shared with the council. The Council needs to be well informed that this plan will take several years to develop and bear some fruit. It needs to know what their roles and responsibilities are from the very beginning of the project. The council also needs to be kept informed on both the status of the project and what advances have been made.

City Manager

The City Manager of West Sacramento, is committed to transforming this stigmatized lower social-economic community into the Premiere City of the region.

The City Manager is currently in the *help it happen* stage of this project. He has given direction to staff to aggressively pursue this new venture for the police department. He is personally interested in this project as an opportunity to change the image of the police department of being a reactive organization to being innovative and futures oriented. This project compliments the police department's other major project of community oriented policing and problem solving.

Mayor

The Mayor is a strong political Illustration in the community. He has the ability to influence and sway members of the city council and the business community. The Mayor is currently in a *block change* mode because he views this project as a "nice-to-have" rather than "gotta-have" program for the police department. He is concerned that

the public's perception of this project is that the department is not using its limited resources to fight the violent crime problems on the street.

The Mayor needs to be moved to at least the *let it happen* mode. This will be accomplished by having several meaningful meetings with the Mayor and explaining in detail the advantages that the plan will bring to the city. Also, future goals for the project will have input from the Mayor in addition to having a good understanding of the roles within the concept should be clearly defined. These meetings will hopefully move the Mayor to the *let it happen* mode. As the plan progresses the Mayor may become publicly supportive of the project but for the time being he has chosen to remain in the background.

Chamber of Commerce

The Chamber of Commerce has strong connections with the business community in West Sacramento and the Sacramento region. It is currently in the *help it happen* mode and has a vested interest in promoting any program that would enhance the business community's perspective of West Sacramento. The Chamber of Commerce can be instrumental in assisting the department develop strong inroads to the high-technology community in developing partnerships. The direction of the Chamber has been fairly predictable for the past several years and has been very supportive of the police department. It is important to remember that the make up of the board changes every two years and needs to be constantly involved with both the design, status and direction

of the project. If there are not constant quality communications between the department and the Chamber's support could diminish.

Chief of Police

The Chief of Police was appointed on August of 1993. The Chief is a Command College graduate and has a philosophy that is futures oriented. The Chief took over a department that was torn by labor strife, low morale and suffered though several embarrassing officer terminations.

The Chief is charged with improving labor relations and making the department more open and responsive to the public. He is continuously building bridges and seeking cooperation from other departments in the city to better meet the needs of the community. The Chief believes in holding his people accountable for their actions and encourages self initiative. He has empowered his management personnel to be creative, innovative and to develop a vision of the future regarding law enforcement in West Sacramento.

The Chief is currently in the *help it happen* stage. He is a strong supporter for technological advances in law enforcement and has made it a priority to computerize the patrol division. The Chief has a good understanding of the need for law enforcement to develop improved knowledge, skills and abilities to combat the growing menace of high-technology crime.

Police Captain

The Captain recently was hired from a large Southern California police department in May, 1994. The Captain is currently familiarizing himself with the community and the department. The Captain is a very important member of the department staff The Captain is responsible for the overall operations of the department. All Division Commanders and the Records Manager report directly to him.

He is also a Command College graduate and is futures oriented. The Captain supports the concept of developing a Cyber Cop approach to the increasing problem of high-technology crime. He is currently in the *let it happen* mode and will probably become more supportive as the department stabilizes. The Captain can move from the position of *let it happen* to *make it happen* as he becomes more comfortable with his environment. He considers himself to be a shaker and maker.

Department Lieutenants

The department's lieutenants commitment to this project is imperative to its success or failure. Lieutenants command the two divisions in the organization Patrol, Services and the Special Projects. Collectively, all three lieutenants command respect from both inside and outside the organization. They are also responsible for the day-to-day operations of the department.

The lieutenant assigned to Special Projects is a key actor of the critical mass. His commitment to this project is in the *make it happen* mode. He has been instrumental in

designing parts of the plan and has the necessary interpersonal skills required to bring together people or groups who comprise the critical mass.

Detective Sergeant

The Detective Sergeant's commitment to the project is in the *help it happen* mode. The Sergeant openly supports the concept of creating a Cyper Cop approach to investigating high-technology crime. The Sergeant has outstanding interpersonal skills and can be instrumental in getting the investigators and other officers in the department supportive of the project.

Director of Data Processing

The Director of Data Processing is a very influential individual when the subject pertains to the use of city maintained computers. Since the City's incorporation, he has been responsible for the operation and purchasing of mainframe, mini-mainframe, and personal computer in the city. His department has control of the police department's record management computer system. For the past six months the Special Projects Lieutenant has been working with the Director to improve communications and cooperation between the two departments. The Special Projects Lieutenant has made some significant inroads with the Director regarding information sharing and computer training. The Director of Data Processing is currently in the *help it happen* mode. It is critical that the Director be part of the planning, transition and implementation

component of this project. This relationship needs to be nurtured on both the formal and informal levels in order for the project to move forward.

Transition Management Structure

The West Sacramento Police Department has recently undertaken its second reorganization in the past ten months. This was done by the Chief of Police to maximize the organization's effectiveness and efficiency. All three lieutenants in the department were transferred to command different divisions in the organization This most recent reorganization was done to encourage new thoughts and ideas from members of the existing command staff and new Captain.

A management retreat was held to further discuss roles and responsibilities of department staff. The management retreat was followed by a team building workshop. At the conclusion of the team building workshop an after action report was prepared assigning responsibility and dates for follow up and tracking of action items identified.

Responsibility Charting

Responsibility charting has been utilized by this project with the goal of clarifying role relationships for those individuals involved with the project. It is a means of reducing ambiguity, wasted energy, wasted time, and adverse emotional reactions . This

activity also promotes team building because it required the anonymous consensus of the group for establishing program responsibilities. **(Table 5)**

Table 5

Responsibility (RASI) Charting

Actors> / Decisions or Acts	Chief of Police	Capt.	Dept. Lt.'s	Project Manager	Dir. of D. P.	Chamber Rep.	City Manager
Develop policy	A	S	S	R	S	S	I
Create a work group to support the Strategic plan and Mission	I	A	S	R	S	I	I
Select the task force	I	S	S	R	S	I	I
Select task force chair	A	R	S	I	I	I	I
Develop team building workshops	I	S	S	R	S	S	I
Develop informal memorandums of understanding with participants	I	S	S	R	S	S	I
Monitor program and business community reactions	I	I	I	R	I	R	S
Progress reports	A	I	I	R	I	I	I
Maintain contact with stakeholders	S	S	S	R	S	S	S

Legend

R = Responsibility for action (but not necessarily authority)
A = Approval (must approve, has power to veto the action)
S = Support (has to provide resources, but does not have to agree to the action)
I = Inform (must be informed before the action, but cannot veto)

Implementation Technologies

Step One

The Chief of Police is one of the key ingredients in the recipe that will facilitate the successful start of the project. The Chief needs to meet with his management staff and share his vision of the project. He has to create a passion in the department on how it is going to undertake this endeavor. He needs to develop one or several strategies with his management team. This strategy needs to be presented to the rest of the department as a unified front on how the department will combat high-technology crime in the future. Roles and responsibilities need to be established at this time to ensure accountability from the onset of the project. A strong sense of unit identity needs to be established. There needs to be an established process of frequent and timely awards. The Chief needs to tell the members involved in this effort that there is an emphasis on self development and improvement. The Chief needs to identify the Project Coordinator who will be responsible for developing the organization's plan.

Time Line

This component of the project should be accomplished within the first month of the project.

Step Two

The second step in this transition process is for the Chief and the Project Coordinator to meet with members of the department's core group to develop a solid foundation of understanding the complexities of this planning and transition process. This group will be challenged to inspire others in the organization to become actively involved with the project by facilitating the spirit of teamwork and making work enjoyable. Initially, the current or present status of the department will be discussed. This group will review the current computer capabilities on the department and reevaluate the quality and types of computer training members of the department have received.

Time Line

Four months have been established as the time line to implement this component of the plan.

Step Three

Step three of this process involves this core group to get together with the key contact persons of city government, the police department, private businesses and other law enforcement agencies. This group also needs to collect and collate all information received from the various internal and external resources in order to establish a concise and workable strategy. Brain storming or nominal group technique processes should be used by this group of people to generate additional ideas of how the details of the project

should be strategized, designed and implemented. This would give this group a feeling of ownership towards the project and ensure a deeper commitment. This endeavor will be both meaningful and facilitate a common vision and shared values.

Time Line

This phase of the implementation plan should take approximately three months to develop and implement.

Step Four

Step four of the implementation plan is to study, evaluate, and recommend for purchase the type of high-technology hardware will be required to support the mission of this project. These items could include but are not limited to: computers, modems, secure transmission lines, encryption systems, data bases, computer information centers (information super highway), mobile computer terminals, and digital radio/telephone communications. Special attention needs to be given to the technologically advanced software needs of the project. Other members in law enforcement, municipal government and private sectors need to be informed and educated regarding this project to expand further system buy-in.

Time Line

Parts of this phase could begin in step three of the project. It will take approximately six months to purchase the required hardware and software necessary for the project. Additional time may be required to learn the programming requirements of the system.

Step Five

The fifth step of this transition process involves training the members of the project in their future roles and responsibilities. They also need to be advised that the strategies developed for this project are fluid and subject to change and further innovation. That much of the future regarding the investigation of high-technology crime is also unknown and is in a constant state of change. The Project Manager (make change happen) will challenge them with the fact that they are the first generation of Cyper-Cops and that all eyes are on them. The implementation of the project begins during this phase. The establishment of an evaluation system for the strategies used in this transition period needs to be developed. The Project Manager will monitor, evaluate and facilitate necessary adjustments also during this phase.

Time Line

This phase of the project should take approximately three to five years to fully accomplish.

SECTION V: CONCLUSIONS AND FINAL COMMENTS

Conclusions

The purpose of this section is to answer the issue and sub-issues raised by the literature review addressed in the first section of this report. These questions will be answered one-by-one in the material immediately below.

How will medium-size law enforcement agencies investigate high-technology crime by the year 2003?

Medium-size law enforcement agencies must develop partnerships with other law enforcement agencies and the private sector in order to effectively investigate high-technology crime in the future. Most medium-size law enforcement agencies are limited in the number of qualified personnel who have a good understanding of computers and the applications of high-technology. Research indicates that larger law enforcement agencies, including the FBI and the California Department of Justice, are also limited in their ability to properly investigate this type of crime.

Medium-size law enforcement agencies will utilize the "team " approach in investigating high-technology crime in the future. No single agency internally has the expertise to investigate the myriad of high-technology crimes. Futhermore, by its very nature, computer-related crime tends to cross jurisdictional and even state and national boundaries. An individual agency may have personnel who have a good understanding of how IBM compatible personal computer systems operate and can investigate crimes

involving that type of hardware. But the same agency would be at a loss in investigating high-technology crimes involving mainframe or Apple computers because no one in their organization is familiar with the respective operating systems. In addition, their personnel will probably need outside assistance in gaining access to information stored on a hard disk that has been pass word or encryption protected.

It will be very important for these medium-size law enforcement agencies to be aware of the resources available to them in investigating high-technology crimes. Organizations such as Search Group, the FBI, Computer Emergency Response Team (CERT), Carnige-Mellon Institute Pittsburgh), VISA security, and the High-technology Crime Investigators Association are available to assist local agencies with these types of specialized investigations. Investigative networks focusing in the area of high-technology crime investigation are also a viable solution that medium-size law enforcement agencies can explore.

At the same time, it is also true that medium-size law enforcement agencies will continue to investigate high-technology crimes with traditional types of investigative techniques well into the year 2003. Law enforcement agencies need to continue to utilize proven investigative techniques when investigating high-technology crimes as long as these techniques are applicable to individual cases. These agencies have utilized their department computer gurus to take the lead in investigating these crimes and will continue to do so in the future. Law enforcement agencies should send this first generation of Cyber Cops to formal training in high-technology crime investigation. This will the first step in developing a solid foundation for future investigative expertise in the

organization. Interview and interrogation skills of the trained investigator will continue to be an invaluable tool in these types of investigations. The use of informants and intelligence information (larger and more inclusive data bases) will also continue to be an important tool for the investigator.

The seizing and examination of evidence will prove to be the weak link in a medium-size law enforcement agency's ability to investigate high-technology crimes. These agencies may need to retain the services of an individual or organization that is trained in high-technology criminal forensics. This is an area in which most medium-size, for that matter large, law enforcement agencies lack the expertise and resources to properly seize, secure and examine both the hardware and software contained in computers and other high-technology devices.

What types of training will be necessary for medium-size law enforcement agencies to properly investigate high-technology crime by the year 2003?

All law enforcement officers in medium-size law enforcement agencies should be trained in the basic high-technology crime investigative skills by the year 2003. It should be clarified that this training is not intended to teach the officer word processing or basic disk operating system (DOS) skills. Officers need basic training in how to identify crimes such as electronic fund transfer fraud, computer scams and the applications of high-technology to every day crimes. This basic high-technology crime investigation

training will heighten the officer's awareness and understanding of a growing problem and give them the necessary skills to properly investigate it in the future.

Computer crime scene investigation or high-technology forensics is an area that needs to be developed as a science. The colleges and universities need to explore the development of a specialized curriculum in this high-technology arena to assist law enforcement. Courses should be made available to law enforcement at both the advance officer training and baccalaureate levels.

Medium-size law enforcement should train their officers in some of the basic skills of how to properly seize and store computers, disks and other peripheral equipment. Should sophisicated computer criminals develop self-destructive programs in computers used in computer-related crimes, an unsuspecting officer could inadvertently destroy evidence stored in that computer. Specialized training will be definitely needed in this area in the future.

There also needs to be some level of training in high-technology crime investigation provided at the supervisory, middle management and executive levels of law enforcement. This training would be primarily intended to increase the level of high-technology crime awareness to a generation of supervisors and managers who have little or no experience in this area. It is hoped that this training or exposure will assist them in promoting and developing programs that will effectively manage this future problem and enable them to provide investigators with the backup they need in their investigations.

What will be the relationship among law enforcement, the educational community and the private sector in investigating high-technology crime by the year 2003?

The key word with respect to this sub-issue is partnerships or synergism. Law enforcement must develop partnerships with the educational community and the private sector in the next ten years. These partnerships will enable agencies of all sizes to call on the expertise of both the educational and private sectors in the investigation of high-technology crime. As early as September 1994 the University of California at Riverside, College of Engineering and Computer Science has been working with both the Commission on Peace Officer Standards and Training (POST) and the California Department of Justice in exploring its potential role could be in the area of education and high-technology crime investigations and applications.

POST in conjunction with the California Department of Justice has scheduled a meeting in Sacramento in January 1995 to discuss issues regarding technology as it relates to law enforcement. Policy makers, at the highest levels, in both education and law enforcement have already began preliminary discussions in developing strategies for meeting law enforcement's technological needs in the next century.

The private sector has been actively involved in organizations such as the High-technology Crime Investigators Association both at a local level and national level. Dean Susan Hackwood of the University of California at Riverside told this researcher that the private sector will always be the front runner in high-technology research and development. Hackwood said that law enforcement needs to work closely with the

private sector in order to keep up with current trends and technologies involving high-technology crime applications.[25]

The private sector wants law enforcement to play a more active role in the investigation of high-technology crime according to Donn Parker. There needs to be improved communications established between the two respective sectors. Law enforcement, in the future, needs to develop more expertise in this area so that the private sector's confidence in law enforcement's ability to investigate high-technology crimes is enhanced.

All parties involved will need each others active participation to develop strategies, programs and training to meet law enforcement's future needs in high-technology crime investigations.

What level of criminal investigations will medium-size law enforcement agencies be responsible for in the investigation of high-technology crime by the year 2003?

The level of criminal investigations will vary from one agency to another depending on the capabilities of that agency. Many medium-size law enforcement agencies in California will have basic high-technology investigative skills by the year 2003? It is quite conceivable that private investigation companies may contract with small and medium-size law enforcement agencies to either conduct the entire investigation or act as a consultant to that agency. In the future, if medium-size law enforcement agencies do not develop the internal expertise to investigate such cases the

private sector may fill that gap. However, medium-size law enforcement agencies may choose to hire consultants as an option due to personnel hiring restraints and reduced budgets. Medium-size law enforcement agencies will continue to be responsible for investigating all local high-technology crimes that occur within their jurisdictions with the exception of cases involving federal crimes.

The Department of Justice will become more directly involved with investigating high-technology crimes in the future. This will partly be due to pressure created by local law enforcement agencies requesting assistance in this area. High-technology companies and large businesses in the state will place a significant amount of political pressure or the legislature and governor's office to increase efforts in investigating this crime of the future.

Final Comments

This research effort that has revealed several interesting issues regarding the investigation of high-technology crime. Law enforcement, in general, is not adequately prepared to effectively investigate most high-technology crimes. One of the aspects of this type of crime that limits law enforcement's ability to investigate this type of crime is that it is ill defined. At present neither within the public nor private sectors is there a standard definition of high-technology crime. Because of this lack of definition it is virtually impossible to have valid statistics on this current and future problem

The FBI has a definition of computer-related crime that fits its need for attacks on major governmental and financial computer systems. This definition does not adequately fit the needs of state and local law enforcement agencies and the private sector in defining high-technology crime.

The private sector lacks confidence in law enforcement's ability to investigate high-technology crime by the private sector. According to industry experts many private companies have not reported high-technology crimes because law enforcement appears reluctant to become involved in those lenghty investigations. Law enforcement is perceived to be intimidated by the use of computers to commit crimes.

Traditionally, law enforcement has trained its officers in the proper methods of investigating crimes by sending them to specialized schools. Examples of this are the homicide and sexual assault schools that many investigators attend. Few investigators,

especially from medium-size law enforcement agencies are being sent to high-technology crime investigation schools.

The capabilities of law enforcement's ability to investigate high-technology crime is hit and miss across a wide spectrum of levels. Even within the FBI, in some parts of the country the local district office may have excellent capabilities of investigating this particular type of crime. In an adjacent district office it may have little local expertise and depend solely on Washington's support for their investigations. The FBI has the good fortune to have the Washington office to support their operations, a luxury not enjoyed by mid-sized law enforcement agencies in California.

Local law enforcement agencies in California are also hit and miss in its ability to investigated high-technology crime. Some of the larger agencies such as the San Jose Police Department have excellent investigative staffs that specialize with this type of investigation. There are also several medium-size agencies such as the Yolo County District Attorney's Office, that have very good capabilities in investigate high-technology crime.

Why do some agencies have a better ability than others to investigate this type of crime? Many of them already have officers employed by their agencies that have both the aptitude and drive to direct these types of investigations. Research indicates that agencies will use in house officers that are computer literate and have an interest in high-technology crime for these types of investigations. These home grown experts are the vanguard of the Cyber Cops of tomorrow.

It was somewhat surprising that there were not more criminals taking advantage of high-technology to commit crimes involving credit card and phone fraud. The opinion of the subject matter experts was that the criminals were not likely to use high-technology when a low technology method was available. They further stated that there will be an increase in both the amounts and complexity of high-technology crimes committed when low technologies are taken away from the criminals. An example of this is illustrated with the crime of credit card fraud. Criminals need the account numbers from the credit card to use it illegally and can often obtain it from copies of bills passing through a merchant or bank administrative offices. It would take a high degree of sophistication to gain access to the bank's data base which has the card's account information. The criminal does not need to use high-technology to get the account number when he/she can get it from a carbon paper that was thrown into the merchant's garbage can. As the bank's use higher technologies that render carbon copies obsolete, for transactions the criminal is forced to also use higher technologies to commit the crime.

High-technology crimes and computer applications are changing at a very rapid pace. They will continue change at a more even faster pace in the next ten years. This researcher has continually updated the introduction portion of this paper in an attempt to keep the project on the cutting edge of information, but it is probable that the material in the introduction may well be out of date within months of the publication of this document. Most certainly, much of the information discussed in this project will be dated within the next year.

It may be of interest to note that several of the events the Nominal Group Technique Panel forecast two years ago have already occurred. These events actually happened three to five earlier than was originally forecast. The message is, the pace of technology is moving more rapidly than the experts thought it would.

Some of the high-technology crime problems that plague law enforcement today will probably be solved by the same technologies that created them. An example of this is the high-technology solution to credit card fraud. Within the near future, according to VISA securitiy, VISA will be using an encrypted bank code that is combined with the individual's personal identification number. This will make it more difficult for criminals to counterfeit the card. In the future, computers with artificial intelligence will be used to assist law enforcement in investigating and solving these high-technology crimes.

The investigation of high-technology crime will continue to be a challenge for law enforcement in the future. The reduction of low technology crimes will bring about a higher number of high-technology crimes committed. Criminals, in the past,used gloves to get around leaving fingerprints at the crime scene. Criminals, in the future, will use computers to committ crimes hoping to leave no electronic fingerprint evidence for investigators to find. Law enforcement must work with other organizations, public and private, in developing partnerships to properly investigate this type of crime in the future.

Endnotes

[1] William S. Sessions, "Computer Crimes: An Escalating Crime Trend," FBI Law Enforcement Bulletin, February 1991, 12-15.

[2] Ibid.

[3] Lawrence F. Young, D. Sc., J. D., "Utopians, Cyberpunks, Players, and Other Computer Criminals: Deterrence and the Law", in Proceedings of the IFPI TC9/WG9.6 Working Conference on Security and Control of Information Technology in Society (on board M/S Llich and ashore at St. Petersburg, Russia, 12-17 August, 1993), ed. Richard Sizer, Louise Yngström, Simone Fischer-Hübner, 186-187.

[4] Ibid.

[5] Fred B. Cotton and William R. Spernow, "Computer Crimes: Scope of the Problem, Search Group, 1993, .

[6] Search Group, Computer Fraud and Theft by Computer, presentation for the California Reserve Peace Officers Association Annual Conference, September 25-26, Sacramento, CA.

[7] Ibid.

[8] J. J. Bloombecker, "Short-circuiting computer crime," Datamation, vol. 35, October 1, 1989, 71.

[9] August Bequai, Technocrimes, Lexington Books, Lexington, Mass., 1987, 45-46.

[10] Richard D. Morrison, "Credit Card Fraud; Crime Does Pay," Law Enforcement Technology, October 1994, 94-97.

[11] Ibid.

[12] US, Department of Justice, Computer Crime, Electronic Fund transfer Systems and Crime, July 1982, vi.

[13] Search Group, Computer Fraud and Theft by Computer, presentation for the California Reserve Peace Officers Association Annual Conference, September 25-26, Sacramento, CA.

[14] Bill Montague and Philip Fiorini, "Privacy abuse "confirms the worst fear"," USA Today, 20 July 1994, 1A.

[15] Mark Lewyn, "Phone sleuths are cutting off the hackers: corporations and phone companies join to end long-distance fraud," Business Week, July 13, 1992, 134.

[16] Donn Parker, "Seventeen Information Security Myths Debunked", in Proceedings of the Sixth IFIP International Conference on Computer Security and Information Integrity in Our Changing World (Helsinki, Finland, 23-25 May, 1990), ed. Klaus Dittrich, Seppo Rautakivi, Junhani Sarri. 363-370.

[17] Keith W. Strandberg, "Thin Blue Line Must Infiltrate On-line Criminals," Law Enforcement Technology, November 1993, 28-32, 51-52.

[18] Philip M. Stanley, "Computer Assisted Investigation Of Computer Crime", in Proceedings of the Sixth IFIP International Conference on Computer Security and Information Integrity in Our Changing World (Helsinki, Finland, 23-25 May, 1990), ed. Klaus Dittrich, Seppo Rautakivi, Junhani Sarri, 389-402.

[19] Evan I. Schartz, Jeffrey Rotherfeder, Lewyn, "Viruses? Who are gonna call? Hackbusters (computer crime)," Business Week, August 6, 1990, 71.

[20] Fred B. Cotton and William R. Spernow, personal interview, Sacramento, CA, 15 January 1993.

[21] August Bequai, Technocrimes, 46.

[22] August Bequai, How to Prevent Computer Crime: A guide for managers, John Wiley and Sons, New York, NY, 137.

[23] Ibid.

[24] August Bequai, Technocrimes, 45.

[25] Susan Hackwood, personal interview, Riverside,CA, 22 September 1994.

Bibliography

Associated Press, "Hacker's racist message heats up Internet", Sacramento Bee, 19 October 1994.

August Bequai, Technocrimes, Lexington Books, Lexington, Mass, 1987.

August Bequai, How to Prevent Computer Crime: A guide for managers, John Wiley and Sons, New York, NY, 1983.

Jane Bird, "Inside Track On Hackers", Management Today, June 1992.

J. J. Bloombecker, "Short-circuiting computer crime," Datamation, vol. 35, October 1, 1989.

Fred Cotton and William Spernow, personal interview, Search Group, Sacramento, CA., 19 January 1993.

Fred Cotton and William Spernow, personal interview, Sacramento, CA, 29 September 1994.

Timothy M. Dees, "A mix of Kids, Computerland Pedophiles," Law Enforcement Technology, October 1994.

John Diamond, "Pentagon can't shake hackers: Intruders still gain access to unclassified computer file," Associated Press, reprint Sacramento Bee, 22 July 1994.

IFIP International Conference on Computer Security and Information Integrity, Proceedings of the Sixth IFIP International Conference on Computer Security and

Information Integrity in Our Cahanging World (Helsinki, Finland, 23-25 May, 1990), ed. Klaus Dittrich, Seppo Rautakivi, Junhani Sarri.

M. Jackson, "Protection of the proprietary information of organizations in the Asia-Pacific Region," in Proceedings of the IFPI TC9/WG9.6 Working Conference on Security and Control of Information Technology in Society (on board M/S Llich and ashore at St. Petersburg, Russia, 12-17 August, 1993), ed. Richard Sizer, Louise Yngström, Simone Fischer-Hübner.

Susan Hackwood, personal interview, Riverside, CA, 22 September 1994.

Eugene Illosvosky, personal interview, Sacramento, CA, 19 October 1994.

International Federation for Information Processing, Proceedings of the IFPI TC9/WG9.6 Working Conference on Security and Control of Information Technology in Society (on board M/S Llich and ashore at St. Petersburg, Russia, 12-17 August, 1993), ed.Richard Sizer,Louise Yngström, Simone Fischer-Hübner.

Barbara Kantrowitz, "Child Abuse in Cyberspace: Child Molesters using computer bulletin boards," Newsweek, vol. 123, N16, 18 April 1994.

Mark Lewyn, "Phone sleuths are cutting off the hackers; corporations and phone companies join to end long-distance fraud," Business Week, 13 July 1992.

Linda Marsa, "High Tech Detecting: The case of magnetic fingerprints", Omni, vol. 17, N1, October 1994.

Deirdre Martin, "Fighting Computer Crime," Law Enforcement Technology, October 1993.

John McKnight, telephone interview, 1 November 1994.

Bill Montague and Philip Fiorini, "Privacy abuse "confirms the worst fear"," USA Today, 20 July 1994.

Richard D. Morrison, "As a matter of Fax: The Fax of the Matter," Law Enforcement Technology, October 1994.

Richard D. Morrison, "Credit Card Fraud; Crime Does Pay," Law Enforcement Technology, October 1994.

Donn Parker, "Seventeen Information Security Myths Debunked", in Proceedings of the Sixth IFIP International Conference on Computer Security and Information Integrity in Our Cahanging World (Helsinki, Finland, 23-25 May, 1990), ed. Klaus Dittrich, Seppo Rautakivi, Junhani Sarri.

Donn B. Parker, telephone interview, 30 September 1994.

Evan I. Schartz, Jeffrey Rotherfeder and Mark lewyn, "Viruses? Who are we gonna call? Hackbusters (computer crime)," Business Week, 6 August 1990.

Robert Schifreen, "Big Brothers Protection Racket: US Government introduces Clipper Chip to Curb Data Hacking," Electronics World and Wireless World, v 100, N1698, May 1994.

Search Group, Computer Fraud and Theft by Computer, Presentation for the California Reserve Officers Association Annual Conference, September 25-26, Sacramento, CA.

Willian S.Sessions, "Computer Crimes: An Escalating Crime Trend," FBI Law Enforcement Bulletin, February 1991.

Murray Slovick, "The Big Brother Chip," Popular Mechanics, September 1994.

Keith W. Strandberg, "Thin Blue Line Must Infiltrate ON-On-line Criminals," Law Enforcement Technology, November 1993.

Philip M. Stanley, "Computer Assisted Investigation Of Computer Crime", in Proceedings of the Sixth IFIP International Conference on Computer Security and Information Integrity in Our Cahanging World (Helsinki, Finland, 23-25 May, 1990), ed. Klaus Dittrich, Seppo Rautakivi, Junhani Sarri.

U.S. Department of Justice. July 1982. Computer Crime, Electronic Fund transfer Systems and Crime,Washington: GPO.

Donn B. Parker, telephone interview, 30 September 1994.

Betsy Wade, "Are you watching your credit cards?", New York Times, The Sacramento Bee, 7 August 1994.

David Wilson, "Computer Insecurity: Computer hackers break into Internet," Chronicle of Higher Education, vol, 40, N24, 16 February 1994.

Lawrence F. Young, D. Sc., J. D., "Utopians, Cyberpunks, Players, and Other Computer Criminals: Deterrence and the Law", in Proceedings of the IFPI TC9/WG9.6 Working Conference on Security and Control of Information Technology in Society (on board M/S Llich and ashore at St. Petersburg, Russia, 12-17 August, 1993), ed.Richard Sizer,Louise Yngström, Simone Fischer-Hübner.

APPENDIX

Appendix A

Issue Focus Panel

Captain Scott Berry, a Patrol Division Commander with twenty years of municipal police experience.

Lieutenant George Brown, a Patrol Division Commander with over twenty-one years of municipal police experience.

Sergenant Russell Thomas, a Patrol Sergeant with over fifthteen years of municipal police experience.

Appendix B

Norminal Group Technique Letter

Dear

Thank you for agreeing to participate in my project of the California Peace Officers Command College. The Command College is a two year masters degree program for law enforcement executives throughout California.

Our panel meeting is scheduled for at 8 A.M. at the California Truckers Association's headquarters building at . (I have enclosed a map of the location and parking is available at the site) The exercise will take approximately 4-5 hours based on prior panels I have participated in the past. At the conclusion of the exercise I would be pleased if you would be my guest for lunch at a local restaurant.

The function of the panel will be to perform a process called the Nominal Group Technique (NGT). In addition to this structured process to develop lists of trends and events, you will be doing some future forecasting. It will be a step by step process, with each step building on the prior step.

The issue we will be concerned with is:

ISSUE:

What affect will high technology crime have on small to medium size law enforcement agencies by the year 2003?

Sub issues:

What changes in criminal law will be necessary to successfully prosecute criminals of computer crime by the year 2003?

What types of training will be necessary for law enforcement to properly investigate computer crime by the year 20003?

What will be the relationship between the private sector and law enforcement in investigating computer crime by the year 2003?

What will be the economic advantage (profit) for law enforcement agencies to investigate computer crime by the year 2003?

You will be asked to list trends and events related to the above described issues. An *event* is a single occurrence, that can be traced to a given point of time. Several events over a period of time is a *trend.* Example: (*Event*) A Boeing 747 crashes at LAX. (*Trend*), a Boeing 747 crashes every Tuesday for a month. Event, the City declares bankruptcy. Trend, the City has had a deficit for three years.

Please think about the issues and possible events or trends and what might affect them in the next ten years. No idea is beyond our limits, so let your imagination run wild.

I know you find the discussion interesting and your contribution will be a positive learning experience for all those in attendance.

Please call me if you have any problems, concerns or are not able to attend on

Sincerely yours,

Lt. Bruce Muramoto
Uniform Services Division Commander

Appendix C

Candidate Trends

1. New operating computer system
2. Criminal computer cases
3. Encryption systems
4. Funding for resources
5. Police officer education
6. Criminal law change
7. Organized crime
8. Public/Private partnerships
9. Asset forfeiture
10. Suburban/rural crime
11. Privacy issues
12. Recruit computer specialist
13. Crime reporting re:computers
14. Large data bases
15. Violent computer crime
16. Officer computer training
17. Use of consultants for investigations
18. Computerized crime scenes
19. Cyber-cops
20. Hackers
21. Crime reporting
22. Computer evidence
23. Computer crime victims
24. Schools/hospitals victims
25. Jurisdictional boundaries
26. Location of computer crime
27. Domestic technology
28. Rapid change in technology
29. Public/private sector competition
30. Evidence code change
31. Civilian computer investigations
32. Computerized information
33. Juvenile computer criminals
34. Computer language skills

Appendix D

Candidate Events

1. Counterfeit identification
2. Hacker disrupts hospital computer, patients die
3. Child pornography
4. Coded encryption used by criminals
5. New bank accounts on-line
6. High technology employees leave US
7. Technology leak gives nuclear bomb to Korea
8. Investigating high technology crime
9. Crimes series
10. Asset seizure law for computers
11. POST required high technology training
12. Private funding for training
13. Victim chosen via electronic bulletin board
14. Law enforcement partnerships
15. Terrorist attack on air traffic control computer
16. Smart Cards replace currency
17. Software made counterfeit securities
18. Personal identification number
19. Legislation passed that prohibits seizure of computers
20. New law requiring on site inspections
21. Civil suit won prohibiting computer readable public record data
22. Hacker stores stolen information in city computer
23. Mandated training for judges
24. Proposition 13 overturned
25. High technology entry level skills for police officers
26. Untrained police employee causes millions of dollars loss in high technology case
27. Police funding depleted by welfare costs
28. Legislature increases penalties for crimes involving use of high technology
29. New law links public/private computer systems
30. Chief solicits funds from private sector for training
31. Global organization investigate computer crime
32. New crime not covered by codes
33. Espionage ring steals company secrets
34. Miranda warning required in language of suspect
35. Elsur rule applicable to local agencies
36. High technology personal phone number for life
37. State computer tax to fund training
38. Small country establish electronic Swiss bank account

TREND EVALUATION FORM

TREND STATEMENT	LEVEL OF THE TREND (today = 100)			
	Five Years Ago	Today	5 Years From Now	10 Years From Now
		100		
		100		
		100		
		100		
		100		
		100		
		100		
		100		
		100		
		100		

EVENT EVALUATION FORM

EVENT STATEMENT	YEARS UNTIL PROBABILITY FIRST EXCEEDS ZERO	PROBABILITY		IMPACT ON THE ISSUE AREA IF THE EVENT OCCURRED	
		Five Years From Now (0-100)	Ten Years From Now (0-100)	Positive (0-10)	Negative (0-10)

FRWB08