

HOW WILL INTERSTATE CYBERFRAUD BE PROSECUTED BY 2006?

A project presented to
California Commission on
Peace Officer Standards and Training

By

Michael Donovan, Chief
Bureau of Investigation
Office of the District Attorney
County of San Bernardino

Command College Class XXXI

Sacramento, California

November 2001

This Command College 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 this Command College project are those of the author and are not necessarily those of the Commission on Peace Officer Standards and Training (POST).

© 2001

California Commission on Peace Officer Standards and Training

TABLE OF CONTENTS

	Page
LIST OF TABLES	iii
ACKNOWLEDGEMENTS	iv
Chapter I	
ISSUE IDENTIFICATION	1
Introduction	1
Statement of the Issue	6
Literature Review & Expert Interviews	7
Chapter II	
FUTURES STUDY	14
Nominal Group Technique	14
Trends	15
Trend Analysis	17
Trend Discussion	18
Events	24
Event Analysis	26
Event Discussion	27
Cross Impact Analysis	32
Alternative Scenarios	36
Scenario One: Optimistic	36
Scenario Two: Pessimistic	37
Scenario Three: Normative	39
Chapter III	
STRATEGIC PLAN	42
Introduction	43
Weaknesses	43
Opportunities	44
Threats	44
Strengths	45
Stakeholders	45
Snaildarters	48
Strategies	48

Chapter IV	
TRANSITION MANAGEMENT	52
Introduction	52
Stakeholders	52
Plan Elements	51
The Importance of Planning	53
Chapter V	
CONCLUSION	56
Introduction	54
Leadership Implications	56
Budgetary Implications	58
Evaluation Activities	59
Recommendations	59
Conclusion	60
THE APPENDICES	
Appendix A	
Nominal Group Technique Panel	62
Appendix B	
List of Trends	63
Appendix C	
List of Events	66
ENDNOTES	68
BIBLIOGRAPHY	69

LIST OF TABLES

Tables		Page
1	Trend Evaluation	16
2	Trend Analysis	18
3	Event Evaluation	25
4	Event Analysis	27
5	Cross Impact Analysis	34

ACKNOWLEDGEMENTS

Command College is like many endeavors. It starts with a single step like any ordinary journey. Along the way, you are introduced to many ideas and innumerable opinions. You meet colleagues and develop friendships, and toil under the burden of coursework. The encouragement and support of many patient people contributed to my successful completion of Command College. It is with gratitude for the endless support of these individuals that I was able to bring my Command College experience to a successful culmination:

The love of my life, my wife Martie

My three sons, Matthew, Mark and Joshua

My District Attorney, Dennis L. Stout

My Chief, Barry A. Bruins (now retired)

My secretary, Claudia Morris

The great members of our team at the San Bernardino County District Attorney's Office

My friends and fellow students from Command College Class XXXI

My Command College Mentor, A.J. "Tony" Sollecito, Huntington Beach Police Department

My Command College Advisor, Dr. Sandy Boyd, Ed.D, College of Marin

My friends at P.O.S.T.

CHAPTER ONE

ISSUE IDENTIFICATION

Introduction

The Internet was developed in the 1960s by a United States governmental agency known as the Advanced Research Projects Agency (ARPA) as a method for universities to communicate with governmental entities regarding weapons research.¹ A key component of the communications network was its redundancy, based on the premise that the communications system could survive in case of nuclear war. The network was able to search communication cables and computers for an expedient method that would guarantee successful communication. If the most direct pathway was too congested or had ceased to exist, such as having the lines cut during a wartime event, the network would simply reroute the communication effort through a different set of cables that would ensure the data reached its destination.²

In the late 1980s and early 1990s, hacking and phreaking came into vogue with the development of personal computers.³ Phreaking denotes the use of computers and illicitly obtained telephone access to commit criminal activity specifically directed at obtaining free telephone time. Teenagers quickly adapted to computer technology and telecommunications. By using computerized bulletin boards, stolen credit card numbers and hacked corporate telecommunication switchboards, this new generation of criminals wreaked havoc on the business community, inflicting hundreds of thousands of dollars of losses. The technology utilized by this new breed of cyber criminal was relatively inexpensive. The most expensive portion of their criminal activity was the purchase of

long distance telephone time, which they actually stole by hacking into corporate communication switchboards.⁴ These criminals developed a culture and their own language.

Hacking activities gave way to more creative criminal acts. Faster computers were required for the expanded activities. Stolen credit card numbers, UPS home delivery and improved computer systems provided the answer. By using a stolen credit card number, telephoning a computer reseller, and then having the equipment shipped to a vacant home, cyber criminals were able to obtain increased abilities.

The introduction of the Internet for business and personal use saw an explosion of cyber crimes taking place via the Internet. Bulletin boards gave way to web sites and e-mail. By the mid-1990s, personal computers were in one out of four homes in the United States. Cyber criminals upgraded their abilities and began terrorizing websites by changing their content or by redirecting the inquiries sent to their web site to a false site established by the hacker. From here, it was a small step to gain access to stolen data and perpetrate vast financial crimes. The theft of information from corporate computers became widespread.

As more and more homes became Internet connected, families began to rely on the Internet as a method by which to conduct business transactions. Home banking through using the Internet gained ground, and purchases by credit card over the Internet became established. Corporate espionage through technological means became standard news, and law enforcement began to realize the cyber criminals held the upper hand. The criminals did not have vehicles that could be chased, and they quickly learned how to

make their cyber activity stealthy and anonymous. Traditional law enforcement measures could not be employed to capture these criminals.

Federal agencies, state agencies and larger local agencies began steps to train law enforcement officials in how to investigate criminal activity involving the Internet, and how to determine the identities of the perpetrators of the cyber crimes. Criminal statutes were written to address utilizing computers to commit criminal acts and to seize the equipment utilized by the cyber criminals to commit their activities. More and more officers attended courses on computer crime and their understanding of conducting the investigations grew.

As officials began to understand how cyber criminals behaved, and how they committed their crimes, gathering evidence to prove the crimes while identifying the criminals became more difficult. Freedom of speech advocates created a website that specialized in providing anonymity to those who desired it. With no requirement that a person using an e-mail account pay a fee or actually disclose his or her true identity, ferreting out cyber criminals became more difficult. Additionally, law enforcement officials began to ask who pays for the cost of the investigations and the equipment necessary to conduct the investigations.

Officials are at a loss as to determine the value of actual losses sustained due to cyberfraud. Officials know that large corporations are routinely victimized, but elect not to report the fraud for fear of generating a negative image of the corporation or a loss of stock value when the public learns of security concerns. There are no reliable statistics on just how many banks have been victimized. So, with no reliable information concerning the number of victims, and no real method by which to quantify losses, the

question is how to identify, prosecute and punish cyberfraud offenders. This is especially disconcerting when some large corporations hire the hackers who terrorized them to defend against other incursions.

Because of the obvious victimization of children, agencies began active investigations into the activities of traffickers of child pornography. Stings were organized where officers pretended to be underage children in cyber chat rooms. On-line conversations were conducted where potential pedophiles were lured across state lines and in some instances across international boundaries to meet and seduce children into sexual activity. Questions began to arise regarding the ethics of importing criminals into a community and expending local resources to prosecute criminals from other states whom, but for the officer's activity, would most likely not have traveled to the jurisdiction where they were arrested.

While law enforcement officials were busy investigating child-focused criminal activity, another area of cyber crime that was virtually exploding was cyberfraud. In cyberfraud cases, large dollar losses are investigated because of the impact such thefts have on our society. In this project, the focus is not the large case, but rather the economics, logistics and legislation of conducting interstate cyberfraud prosecutions.

The Federal government has statutory authority to prosecute crimes that occur over interstate boundaries. Many local law enforcement officials who have dealt with a fraud case have asked the United States Attorney's Office for assistance only to find their plea for assistance goes largely unanswered. Federal authorities cite myriad reasons for their inability to help. Chief among these reasons is the government's base level of economic loss required for their intervention. With the increasing number of interstate

fraudulent activities, the United States Attorney's Office ever increases the dollar loss they require to authorize a federal investigation and subsequent prosecution. Although many prosecutors and law enforcement authorities were interviewed regarding this situation, none were willing to provide a quote for publication. To a person, however, every official interviewed expressed displeasure with the federal authority's unwillingness to assist local authorities with complex criminal investigations and prosecutions.

The result of this ever increasing base economic loss requirement for federal involvement has been to grant cyber criminals the ability to commit cyberfraud with virtual impunity, provided the crimes are committed across state lines. No laws exist which allow local or state officials in one state to prosecute a criminal in another state for crimes generated in a different state. For example, if a cyber criminal in Maine sells a Rolex watch over an Internet auction site to a buyer in California, no state criminal statutes have been broken. Once the buyer has paid for the watch, if the watch that arrives from Maine in California is determined to be a fake Rolex, then a criminal act has occurred. The questions that arise are substantial:

- Is the act a civil tort or a criminal act?
- If the activity is determined to have the requisite criminal intent, who has jurisdiction at a local level to prosecute the criminal?
- If the loss is minimal, does the cost of prosecution outweigh the economic loss to the victim?
- Who pays for the extradition, especially in cases where the loss is minimal?

- If the role is reversed and the victim is in Maine and the suspect is in California, who pays the expenses for the witness to travel to California to testify in court?
- Is there a way to use technology to our advantage to reduce costs, ensure the defendant's right to confront and cross-examine his accusers, and to reduce the lure of committing cyberfraud with impunity?

By exploring how cyberfraud will be prosecuted in the future, we can provide acceptable answers to these questions and thus prepare to meet the challenges cyberfraud present to law enforcement.

Statement of the Issue

Interstate cyberfraud is defined as using computer technology to cross the geopolitical boundaries of one state to enter another state for the purpose of committing criminal fraud. The types and descriptions of fraud are as enumerable as the stars, and thus do not bear description here. Any good confidence man can use a computer to his advantage and steal an endless bounty of funds from an unwary victim with virtual impunity as he hides behind the veil of committing interstate crimes via the Internet.

The case of prosecuting cyberfraud activity at hand is that Interstate cyberfraud is largely ignored now, except in large federal investigations. This allows common thieves to operate in a high tech environment with virtual impunity. There is no denying that computers are a part of everyday life, and that in the future, more computers will be put into use. With the growing popularity of the Internet, and the increasing speed at which technology performs, more and more criminals will be taking to the Internet to conduct

their transactions. As evidence of this, all one has to do is look at the rate at which public telephones are disappearing, and the number of adults and children who now have a cellular telephone pressed to their ear. Technology is being embraced at an ever-increasing pace. By developing a plan to address interstate cyberfraud, our citizens can be better protected while ensuring criminals will have to answer for their misdeeds.

By preparing for the future, we can keep from becoming victims of destiny. Addressing the issue of how interstate cyberfraud will be prosecuted in the future (2006) allows us to prepare for and work to construct a desirable future.

Literature Review and Expert Interviews

Personal interviews of experts in the area of high technology prosecutions were conducted, and literature was reviewed in order to determine the present state of the issue in California regarding the ability to prosecute interstate cyber crime. This literature review and the interviews that were conducted is not meant to be exhaustive, but rather to provide insight into California's present readiness to conduct interstate cyberfraud prosecutions, and its potential to develop a future ability to perform such prosecutions.

Although society is becoming increasingly aware of cyberfraud by way of stories in the media, law enforcement authorities remain ineffective in their ability to investigate and prosecute many types of cyberfraud. In his book, High Technology Crime, Kenneth Rosenblatt discusses the issues related to computer crime for almost six-hundred pages.⁵ Rosenblatt points out that in 1991, PBX fraud was approximately \$500 million annually. He further points to hostile computer warehouse takeover robberies and burglaries where millions are stolen from merchants.⁶

After reading Rosenblatt's book, it becomes painfully obvious that there is no one particular methodology to employ for investigating high technology crime, and that any high technology crime investigation is fraught with unresolved legal issues, such as first amendment rights and violation of privacy. Adding corporate espionage and the theft of trade secrets to the mix further complicates the issues, thus making a complex investigation into a technological arena even more difficult.

Identity theft has become popular and promises to be the newest criminal threat to consumers who use technology to conduct their affairs. As of April 1998, it was estimated that one in four adults were victims of identity theft.⁷ In identity theft situations, victims have their social security number stolen by a criminal with ill intent. The thief, using the stolen number, assumes the identity of the victim and creates a credit portfolio using the victim's personal information. In this manner, an individual's credit history is ruined, and next to impossible to repair. Since much of the activity is conducted on-line, tracking the suspect is difficult. When the thief perpetrates the theft via computer over an interstate line, jurisdictional issues become almost insurmountable should the suspect be identified and enough evidence produced to file criminal charges.

Assistant District Attorney Jim Hackleman of the San Bernardino County District Attorney's Office in California deals with cyberfraud jurisdictions routinely. Much to the chagrin of local law enforcement agencies, criminal complaints are routinely turned down because the cost of prosecution far outweighs the value of the theft perpetrated. Therefore, the San Bernardino County District Attorney's Office has established a policy to act as a guideline for prosecuting interstate high technology cases. This policy takes a wait and see approach to interstate cases, attempting to force the issue of federal

jurisdiction on the FBI and United States Attorney's Office, based on the federal jurisdiction of the cases in question.⁸

Hackleman believes that resources are scarce, and in such a scarce environment human resources and capital cannot be spared on interstate cyberfraud. It is Hackleman's contention that pressure must be brought to bear on federal authorities to provide a funding source to deal effectively with interstate cyberfraud. Until such funding materializes, Hackleman takes the position that investigating such matters is a waste of precious resources that could be better allocated elsewhere, as the return on investment is dismal, often costing several times more to prosecute a case than was actually stolen.⁹

Redlands Police Department Deputy Chief of Police Clete Hyman pointed out in an interview that there are very few computer-literate investigators who are capable of conducting a high technology crime investigation. Chief Hyman organized a High Technology Crime Task Force for San Bernardino County. The task force is organized as a high tech SWAT team, composed of investigators from every law enforcement agency in the county who are dispatched on an as-needed basis. This team assembles monthly to conduct continuing education for their members, to develop policies, and to design outreach programs to educate the public and law enforcement on scams to be aware of, and on how to ask the team for assistance.¹⁰

Chief Hyman sees a time in the future where cyberfraud will be so omnipresent that officers and prosecutors will have to be skilled in order to conduct their jobs. At this time, however, such skill sets are rare, and the call for such training is rare. He believes that the team will continue to operate in its present manner until funds from the state or the federal government are made available to fund the team to operate full-time. Absent

such funding, there is insufficient high technology crime reported in San Bernardino County to make funding the team as a full-time entity a priority.¹¹

San Bernardino County District Attorney Dennis L. Stout believes that technology similar to the technology being used to perpetrate interstate cyberfraud can be focused to combat interstate cyberfraud. Stout recently installed smart videoconferencing equipment in his office which allows the camera to track the voice of the person speaking. The purpose of the investment was to allow conferences to take place where Deputy District Attorneys would not have to leave their office to appear at parole hearings, where similar equipment allows the parties at the hearing to see and hear the deputy DA and be seen and heard by the deputy DA at the same time. This system allows high quality image and voice data to be transmitted while reducing time and expenditure commitments necessitated by traveling to distant prisons to appear in person.¹²

If Stout's idea is taken one step further, a network of high definition videoconferencing systems could be constructed that would allow victims to physically appear in a court facility near their home or office and be broadcast to a remote location where a hearing was taking place. This type of system would allow a victim's mannerisms to be studied by jurors, judges and attorneys. Truthfulness could then be assessed just as if the victim were actually in the courtroom. Questions could be asked and answered instantly, and most importantly, valuable resources could be saved while increasing the system's ability to prosecute interstate cyberfraud as well as other criminal violations.¹³

In 1998, the California legislature passed Penal Code section 13848 into law to provide limited funding for the investigation and prosecution of high technology crime.¹⁴ The first such program in the state was the Sacramento Valley High Tech Crime Task Force. This task force used state funding in conjunction with industry funding and agency funding to establish a squad of investigators to focus on technology crimes in the Sacramento area. Although successful, this team focused on the theft of equipment, cloning of cellular telephones and the remarking of stolen computer chips. Remarking chips involves changing their markings so that a chip can be sold as a faster processor than it actually is. The team did not cross state lines to conduct its investigations, limiting its endeavors to the Sacramento area.¹⁵

Even with existing laws and the introduction of newer legislation such as California Penal Code section 13848, peace officers are limited in their authority to conduct investigations into crimes that originate in other states. California Penal Code section 1524.2 only provides California peace officers the authority to execute search warrants in California, and thereby bars California officials from having the power to search computers and criminals in jurisdictions outside the state, thus offering a degree of protection to parties engaging in internet cyberfraud. By working with federal officials, there is a possibility of expanding this to interstate authority, thus giving law enforcement officials better tools with which to investigate interstate cyberfraud.

California Penal Code Section 865 provides that a witness in a criminal matter must be examined in the presence of the defendant, and may be cross-examined in his behalf.¹⁶ This law gives defendants in criminal cases the right to confront and cross-examine witnesses against them, and makes no provision for constructive examination

via live high definition video conferencing. California Penal Code section 866 specifically prohibits authorizing or compelling depositions of witnesses.¹⁷

California law provides a method by which to compel the attendance of a witness to testify in a criminal matter. Witnesses who fail to appear subsequent to being served a lawful subpoena may have a warrant issued for their arrest and be brought before the magistrate in custody.¹⁸ California Penal Code Section 1334 is known as the Uniform Act to Secure Attendance of Witnesses Outside the State, or the Interstate Witness Compact.¹⁹ This section of law was developed in cooperation with virtually every other state in the country to provide for compelling witnesses in a criminal case to attend the trial in another state to testify in person. The code provides immunity while in transit to the state where the trial is being held, as well as immunity from prosecution while in transit to the state in question.

There are very limited times wherein closed circuit television may be utilized to obtain the testimony of a witness in a California criminal matter. According to California law, certain children who are victims of sexual assault may testify via closed circuit television.²⁰ It is a logical inference to extrapolate the use of closed circuit television into the use of a high definition video conferencing system. Therefore, there is some precedent for using live video testimony in California, and the ability to modify this statute or expand the usefulness of this technology by new legislation exists. Such an expansion could provide for the use of this technology in other matters where witnesses reside outside of California.

By reviewing literature on the subject and conducting interviews with experts, it very rapidly becomes clear that law enforcement officials are not all singing off the same

sheet of music. Different jurisdictions have differing guidelines on how they address Internet cyberfraud. Only federal authorities have bona fide jurisdiction to prosecute interstate cyberfraud, and their investigation and prosecution criteria vary from state to state.²¹ This variance in prosecution criteria is due to each regional U.S. Attorney's ability to set priorities for their region based on staffing and funding needs as well as regional crime patterns. Only by investigating and identifying a unified course of action can local and state agencies hope to obtain a useful solution regarding their attempt to investigate and prosecute interstate cyberfraud in the future. The next chapter discusses forecasting the future regarding prosecuting interstate cyberfraud.

CHAPTER TWO

FORECASTING THE FUTURE

Nominal Group Technique

In order to develop a model strategic plan and identify and measure possible trends and events, the Nominal Group Technique (NGT) was utilized. This technique can be used to assist in the creation and management of a desirable future with respect to particular issues.

There were a number of individuals selected to participate on the panel.

- An expert in computer technology and networking who has extensive experience in computer security and computer communications in operating computer networks for the San Bernardino County Sheriff's Department and the San Bernardino County District Attorney's Office.
- The Assistant District Attorney from the San Bernardino County District Attorney's Office, responsible for policy development and implementation regarding the prosecutions of high technology crime and the extradition of criminals from other jurisdictions.
- A Special Agent from the Federal Bureau of Investigation who has a law degree and experience as a former city police officer and Deputy District Attorney and is now tasked with investigating telemarketing fraud.
- A Supervising District Attorney's Investigator from the San Bernardino County DA's Office who is responsible for representing the District Attorney's Office on two county-wide high technology committees that

develop policies, and who has previously supervised the investigation of high technology crime investigations that involved interstate crime elements were included in the panel.

- A Deputy Attorney General who is assigned as a prosecutor for one of the California Department of Justice's high technology regional crime task forces.
- The Deputy Chief of Police of the Redlands Police Department, who is appointed by the San Bernardino County Chiefs of Police to run the county's high technology crime investigation team, develop high technology criminal investigation training, design a public awareness campaign, and oversee the assignment of high technology crime investigations.

Approximately six weeks before the NGT panel met to conduct the NGT process, the panel participants were mailed information describing the NGT process as well as material outlining the scope of the problems involving prosecuting interstate cyberfraud.

Trends

The panel met on Friday, April 13, 2001, in the main conference room of the San Bernardino County District Attorney's Office in San Bernardino. A description of the NGT process was presented. Clarifications were made regarding expectations and time frames for the process. Additional oral material was presented regarding the background for the issue, and the panel was then asked to identify emerging trends that related to the prosecution of interstate cyberfraud. The panel identified fifty-one trends, from which the participants were asked to select the top trends that they believed would have the

largest impact on the issue of prosecuting interstate cyberfraud (Appendix A). This selection was done by oral vote, and an assistant tallied the results. The panel selected nine top priorities from the total of fifty-one identified trends.

Table 1 - Trend Evaluation

	-5 Years 1996	Today 2001	+5 Years 2006	+10 Years 2011	Concern 1-10*
Trend 1: Internet for Commerce	10	100	250	475	8.0
Trend 2: Multiple Jurisdictions	60	100	250	400	8.5
Trend 3: Biometric EFT's	7	100	275	500	6.0
Trend 4: Internet Speed	30	100	200	300	7.0
Trend 5: Prosecutorial Resistance	100	100	120	110	6.5
Trend 6: LE Knowledge of Cybercrime	16	100	275	600	9.0
Trend 7: Public Pressure	8	100	175	300	8.0
Trend 8: High Tech Courtrooms	5	100	225	400	8.0
Trend 9: Identity Theft	35	100	225	375	6.0

*1 indicates **LEAST** concern, 10 indicates **MOST** concern

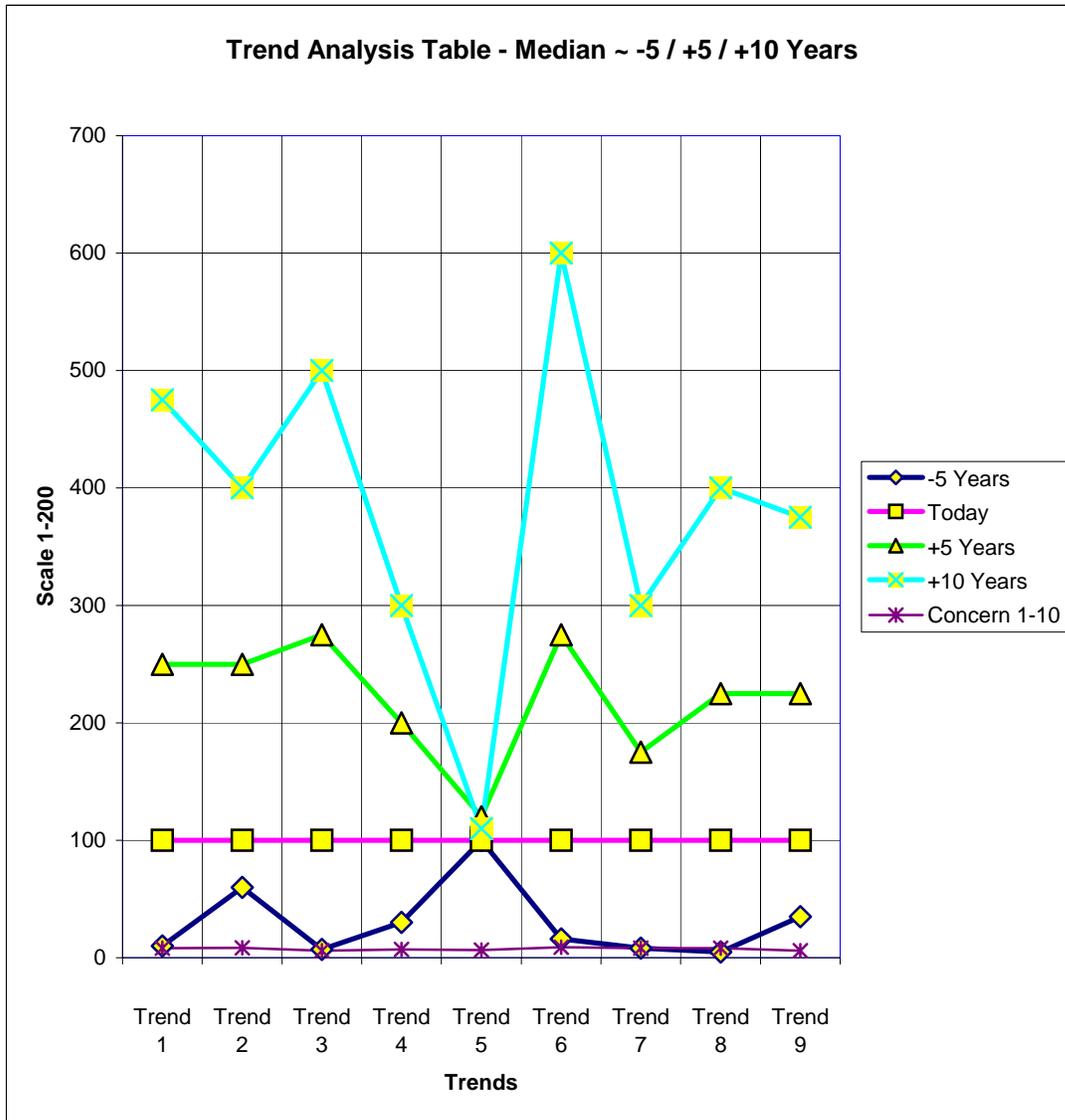
Each of the trends was discussed in detail by the panel. The following information is a summary of the discussions conducted by the panel.

Trend Analysis

Presuming a value of 100 for the present year 2001, The NGT panel participants were next asked to each provide an individual estimate of the value the selected trends had in relation to the present. The trends were ranked for their relevance to the issue five years prior, in 1996, as well as five and ten years hence, in 2006 and 2011. The panel concluded that all but one of the trends had increased since 1996. The panel identified Trend 5, resistance by local prosecutors to handle cyber crime, would actually slightly decrease in the future from 2006 to 2011. For each of the other trends, panelists predicted substantial increases from present to 2011. These increases showed an average perceived increase of one-hundred percent magnitude five years into the future, and an average of three-hundred percent increase from present to ten years in the future.

Table 2

Trend Analysis



Trend Discussion

The NGT panelists discussed the trends in detail. The following list of trends were deemed to have the largest impact on the issue of prosecuting interstate cyberfraud in the future, and are therefore discussed below:

Trend 1: Use of the Internet for commerce.

Society is focused on speed. We require faster responses, more timely communication and quicker delivery of goods and services. Technology is moving away from interacting with individuals for conducting commerce. Some financial institutions are forcing electronic banking by charging additional fees to conduct face-to-face business with a human being. Automated teller cards, check cards and direct deposits to bank accounts are becoming a standard way of doing business. This way of doing business has created a degree of comfort in conducting electronic transactions. Our desire for speed, ease of use and convenience has contributed to an increased demand for electronic commerce that can be conducted over the Internet. Merchants are offering goods and services which are sold over the Internet and paid for via credit cards over the Internet without ever seeing the physical item being sold or the face of the merchant conducting the transaction.

Trend 2: Offenses that occur in multiple jurisdictions.

As the Internet has become an accepted method of conducting business, cyber criminals have the opportunity to victimize individuals in multiple jurisdictions without ever having to travel from their computer. This victimization can be done without regard for state or national borders. By having victims in multiple jurisdictions, investigation and prosecution efforts are confused and often lead to inaction by law enforcement officials. In a recent San Bernardino County case, a decision was made not to prosecute a local Internet salesman who offered Rolex Watches for sale that were not actually Rolexes. It became evident after the initial investigation that the cost of transporting

witnesses from numerous states to testify against the man far outweighed the benefit of prosecuting him.

Trend 3: Electronic fund transfers utilizing biometric-based ID system.

Research is being conducted that will allow the use of genetic material to identify individuals conducting electronic commerce. Existing systems allow for fingerprint recognition and retinal scans as methods of proof of identity for accessing computer systems. Using biometric technology will increase the difficulty of committing electronic fraud, and will give prosecutors evidence of identity by which to prove criminal cases of cyberfraud in court. Some members of the panel believed that a day would come where electronic funds transfers will not occur until some form of bio-identification has confirmed one's true identity. Bio-identification was identified as retinal scans and fingerprints presently, but could include more advanced identification methods in the future.

Trend 4: Speed of the Internet.

Some discussion centered on the increasing speed of the Internet. Moore's Law regarding the doubling of processor speed every 18 months was addressed, as well as technological innovations that will allow faster throughput with regard to Internet connectivity.²² One panelist opined that the Internet would be 30 times faster than today in five years, and 100 times faster than present within ten years.

Panelists believed that increased Internet speeds would allow the implementation of real-time video conferencing in criminal trials. Panelists believed that clear streaming

video would be introduced that would eliminate jittery images as Internet speeds and throughput increased.

Trend 5: Resistance by local prosecutors to handle cyber crime.

Panelists believed that there is presently a chasm of ignorance regarding cyber crime knowledge, and thus a reluctance to prosecute high technology crimes out of fear of the unknown. The panelists believed that as new prosecutors are hired, the fear of high technology would shrink, as new attorneys are accustomed to working with technology due to their having grown up using technology to their advantage. This knowledge will fuel a desire to prosecute cyberfraud as the right thing to do.

Another panelist pointed out that absent additional resources being thrown at the problem of cyberfraud, existing resources would demand status quo attention be paid to cyberfraud. Rapes, robberies and murders will continue to be the bread and butter prosecution effort as cyberfraud will require additional time and energy which will not be available. Given the limited resources, there was a belief that supervisors will not want to spend valuable resources dealing with cyber crime.

Other panelists believed the introduction of new lawyers into the prosecution effort will cause technology to be embraced. New prosecutors will demand technology to solve problems. Panelists believed the introduction of high definition television into courtrooms would allow real-time long-distance video conferencing for prosecution efforts, thus increasing risk taking in prosecutorial efforts. Risk taking in this arena was viewed as a positive aspect of this trend.

Trend 6: Knowledge/awareness by law enforcement of cyber crime.

Panelists believed that there are many law enforcement officers who remain afraid of computer technology, particularly when they are asked to personally interact with the technology. The NGT panel pointed out that this group of employees is diminishing, and that more employees in law enforcement are embracing computers, thus creating a larger number of officers who are willing to investigate computer crime because they understand it, or are willing to be trained in how to investigate it. Ultimately, the panel believes that cyber crime prosecutions will increase as older employees leave law enforcement.

Trend 7: Public pressure for enforcement of cyber crimes.

Panelists believed that public pressure would drive the investigation of cyber crimes. The politics of the activity will necessitate that agencies take an active role in investigating and prosecuting criminal cyberfraud in order to meet the rising tide of public pressure as cyber crime activity increases and the number of victims grows.

Panelists attributed the lack of present pressure and concern regarding prosecution effort to the “out of sight, out of mind” mindset. Most people are not presently directly affected by cyberfraud and therefore are not clamoring for a law enforcement response. Panelists pointed to companies passing the costs of cyberfraud on to consumers in the form of high prices to deal with their losses. There is an opportunity for increased public pressure as prices rise to combat cyberfraud losses.

Trend 8: Electronic High Tech Courtroom.

Panelists believed that as the cost of technology decreases, and the quality of the technology increases, high technology solutions would enter the courtroom. The ability to provide inexpensive prosecutions by using videoconferencing for long-distance testimony will have a substantial allure. The cost savings associated with not having to fly witnesses from out of state to testify will have been embraced as a time and cost saver. The introduction of technology into the courtroom has the potential to revolutionize the way trials are conducted. Potentially more cases will settle outside of court once the defense bar is no longer able to count on expensive travel as a barrier to successful prosecution. Panelists envisioned a day in the future where victims could testify from their home or office and avoid the inconvenience and expense of traveling to distant venues.

Trend 9: Identity Theft.

The NGT panel believed that as public awareness of identify theft increased, and more members of the public become victimized, public outrage will drive prosecution and enforcement efforts. This public outrage would affect changes in law as well as force technological changes that would prevent the effective theft of a person's identity. Panelists believed that the problem with identity theft is growing exponentially and that although it is a huge problem in the United States, expansion of the problem to global proportions will generate huge difficulties. Credit card usage in foreign countries will

contribute greatly to expanding identity theft to the rest of the world as a fashionable crime.

Events

After discussing the trends, the Nominal Group Technique panel next turned its attention to identifying events they believed could occur over the next ten years that could significantly impact on the issue. The panel identified thirty events (Appendix C). The panel voted on these thirty events and determined that nine of the thirty events would have significant impact on the issue of prosecuting interstate cyberfraud.

Table 3

Event Evaluation

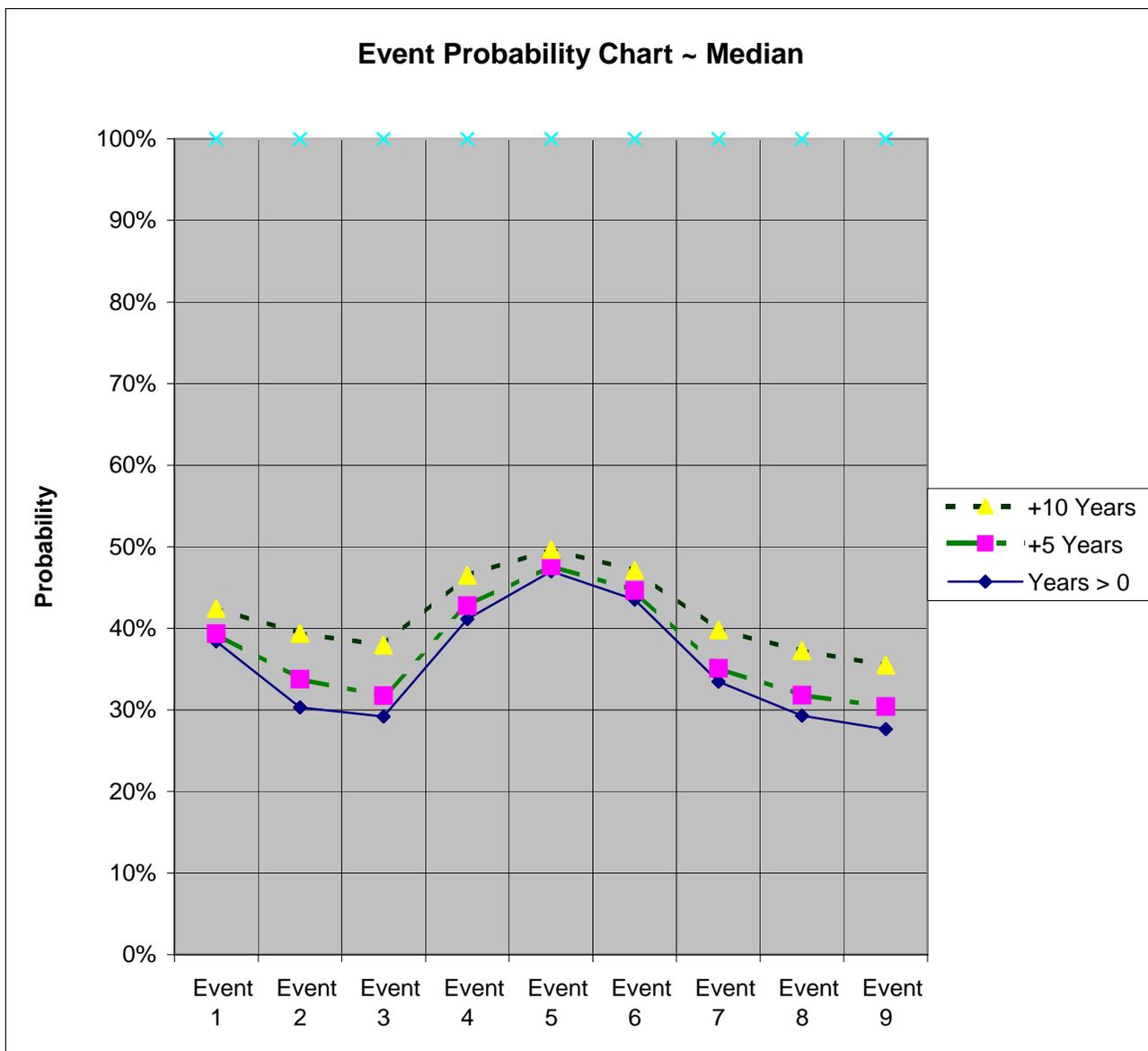
	First Year Event Could Occur	Probability of Event Occurring by 2006	Probability of Event Occurring by 2011	Positive or Negative Impact on the Issue	Amount of Impact (1-10)
Event 1: UN Signs Treaty	2005	15%	48%	+	9.0
Event 2: Forensics Network	2003.5	40%	65%	+	7.0
Event 3: High Tech Courtrooms	2004	35%	85%	+	8.5
Event 4: LE Cross Designation	2005	20%	45%	+	6.5
Event 5: Uniform User ID Act	2007	0%	30%	+	7.5
Event 6: Anonymity Eliminated	2007	0%	40%	+	8.5
Event 7: Biometric e-Commerce	2005	25%	70%	+	9.0
Event 8: Computer Archiving	2003.5	30%	65%	+	7.5
Event 9: Central DB for Industry	2003	30%	55%	+	7.0

Panelists discussed these events in detail after their votes were cast. The following information is a summary of the discussions concerning these events.

Event Analysis

After ranking the events, the NGT panel was asked to determine the first year in which a particular event could possibly occur. As an example, every panelist believed that it would take about five years from 2001 before the United Nations could implement any kind of legislation that would enable the prosecution of cyber criminals. The panel was asked to rank the likelihood of the event occurring five years and ten years hence, or 2006 and 2011. The panelists demonstrated their belief in this likelihood by using a 100-point scale. In the case of the United Nations legislation, the panel believed there was only a 15% chance of such legislation being enacted by 2006. The panel was then asked to determine whether the occurrence of the event would be a positive or negative impact on the issue of prosecuting interstate cyberfraud. In this UN example, the panel determined that enactment of the legislation would be positive on the prosecution effort. Lastly, the panelists were asked to rank every event regarding its impact on the issue of prosecuting interstate cyberfraud, using 1-10, with 10 being the largest impact. In the UN example, the panel determined that the establishment of such legislation would have an impact of eight, meaning the impact was seen as significant. The following table reflects the median values given to the top events by the panel.

Table 4
Event Analysis



Event Discussion

The NGT panelists discussed the events in detail. The following list of events were deemed to have the largest impact on the issue of prosecuting interstate cyberfraud in the future, and are therefore discussed below:

Event 1: UN signs international treaty to allow for prosecution of cyber criminals.

The panelists believed that a standardized encompassing treaty to deal with prosecuting cyber criminals was unlikely based on existing levels of international cooperation. Panelists did, however, believe that the possibility existed for a non-comprehensive effort to establish rules of prosecuting international cyber criminals. Panelists believed that an initial effort in this area could be made by NATO in order to demonstrate the workability and merit of such an idea.

Event 2: Development of a national forensics network.

Panelists pointed to the trend of regional forensics laboratories as making it difficult to establish a national effort in this arena in the short run. The lack of presently existing regional labs, as well as the relatively few national labs, coupled with existing local and national efforts was cited as indicia of what the future holds. One panelist pointed out that we will be forced toward a national model, as the problem will drive the solution as funding and geopolitical boundaries will force federal authorities to establish national labs.

Event 3: High tech court rooms authorized by law.

As courtrooms become busier, technology will have to be introduced to cause the system to work smarter. Panelists believed that a mandate will be made which will force all courts to become immersed in high technology in order to affect their mission. Panelists believed that the American Civil Liberties Union (ACLU) will attempt to derail

any effort to impose technology into the courtroom which will invade our right to confront and cross examine accusers in criminal court.

Other panelists believed that the infusion of technology into courtrooms would be done incrementally, with legislation enabling this to start in civil courts, and then expand in a second phase into criminal courts. Panelists pointed to the nonacceptance of facsimile subpoenas when the technology was in its infancy, and how fax machines and their printed output are now taken for granted. Another panelist envisioned initial forays into the criminal arena by utilizing videoconferencing equipment at preliminary hearings.

Event 4: Cross designation of law enforcement officers between states.

One theory which panelists advanced was a model where law enforcement officers from different states would be cross-sworn to enforce laws in states outside their state of origin. This model is similar to the cross-designation of local police officers as federal officers when they are involved in joint local/federal task forces. Panelists envisioned difficulty in this area as officers from any bordering states have a history of not getting along. One panelist believed that testing the waters by establishing cyber cops with such cross-designated abilities would have success.

Event 5: Uniformed User Identification Act.

Although panelists thought establishing a uniformed user identification act would have broad-reaching affects, they also thought that implementation would be difficult. The specter of Big Brother, infringement on personal liberty, and opposition on the basis of the difficulty of implementation would all come into play. Panelists believed that only

an event of epic proportions would give rise to a public perception that such an act would be required and tolerated. An epic event might be a cyber terrorist hacking into a computer database, pretending to be an authorized user, then taking a power grid offline resulting in the deaths of innocent citizens. Establishing a tracking number would be seen as an attempt to issue an ID number to citizens which would have an impact on various religious elements of our society and might well lead to some degree of anarchy if implementation were attempted.

Event 6: A law eliminating anonymous use of Internet is enacted.

It is presently possible for an Internet user to establish an anonymous identity on the Internet, thus affording the user the ability to surf and e-mail with complete anonymity and thus absolute impunity. A discussion broke out amongst the panelists as to whether using the Internet was a right or a privilege, as in driving a vehicle is perceived as a right but is legally considered a privilege. As technology controls more of our lives, public opinion will shift and give the status of right to Internet usage. It is possible to establish Internet e-mail accounts where you remain anonymous by virtue of websites that cater to users who desire anonymity or via users who provide inaccurate or false identification data when establishing such accounts. As cyberfraud becomes more pervasive, the right to remain anonymous will quickly give way to the right to enforce criminal statutes by determining the identity of the individuals conducting business on the Internet.

Event 7: Biometrics used for e-commerce.

The panel pointed to the existing use of biometrics by industry, citing that Microsoft Corporation has already built such technology into its Windows software. Biometrics technology uses unique body structures, such as fingerprints or retinas as an identification mechanism. Software scans the body part and compares the user's body part against the copy of the part on file. When there is a match, access is granted. Microsoft Corporation has an interface that allows the use of fingerprint scanning technology to ensure a user logging onto a system is the authorized user. The panelists believed that initial consumer usage in this area would surface in the use of biotechnology in credit cards. The cost of using technology is becoming inexpensive, and the use of fingerprint scans may be one of the first usages of biotechnology in this area.

Panelists believed that the government could not force the issue of using biotechnology for identification purposes. Panelists saw industry leading this issue in an effort to control their losses and properly identify consumers to protect everyone involved in commerce. Panelists believed that if biometric usage was driven by industry, little resistance by the public would be encountered.

Event 8: A law is passed to require computer record archiving.

Although this would be a minor inconvenience to industry service providers, the panel saw this as a logical extension of what is presently being done. Panelists pointed to Internet Service Providers who presently archive activity of their users for approximately 30 days. By requiring a 12 to 24 month archive of traffic and message activity, law

enforcement efforts would be greatly enhanced in their ability to conduct investigations and identify suspects committing cyberfraud.

Event 9: Central database established for private industry reports for cyberfraud.

The panelists believed that much of corporate America does not report criminal conduct to law enforcement, effectively hiding many of the crimes that victimize them to prevent public impact on the perception of their firm. Panelists believed that only forcing industry to report crime would paint a true picture of what is occurring. The panel evidenced bank robberies, believing that in many instances, banks would allow robberies to go unreported in order to reduce negative public relations if the banks could figure out a method to avoid the bad press relations. Establishing such a database would provide a clearinghouse for conducting investigations and determining the identity and origin of the attacks, as well as the methodology used to perpetrate the crimes.

Cross Impact Analysis

Trends and events do not occur in a vacuum, and thus, by their very nature, impact upon each other, with events influencing trends. Therefore, in order to more fully understand these impacts, it is necessary to conduct a Cross Impact Analysis. In order to do this, some members of the panel were asked to consider the impact each of their identified events would have on the trends they cultivated. A chart was developed to illustrate the impact. A scale of -5 to +5 was utilized. In this chart, -5 has the most negative impact on the issue, while a +5 indicates the most positive impact on an issue. A zero (0) indicates that there is a neutral impact or effect on the issue.

After the impacts are determined, a strategic plan can be developed in order to attempt to impact future events in as positive a manner as possible, in essence attempting to define a positive future based upon the panel's predictions. In essence, if Event 1 were to happen, and it is predicted to have a positive effect on the majority of the identified trends, then there is a benefit to be derived by fostering an environment conducive to making Event 1 happen. Conversely, if the occurrence of Event 1 causes the majority of trends to be reported as negative values, then benefit is presumably derived by designing a methodology that will prevent Event 1 from occurring.

Table 5
Cross Impact Analysis

	TREND 1	TREND 2	TREND 3	TREND 4	TREND 5	TREND 6	TREND 7	TREND 8	TREND 9
EVENT 1	+2	+1	+5	0	+1	0	+1	+4	+3
EVENT 2	+2	+4	0	-1	0	0	+2	+1	-3
EVENT 3	0	+4	2	+5	+5	+2	+4	+5	+2
EVENT 4	+2	+4	+1	+1	+2	+4	+4	+4	+4
EVENT 5	+5	+2	+3	+1	+2	+2	-2	+2	+5
EVENT 6	+5	+2	+5	+1	+5	+4	+2	+4	+5
EVENT 7	+5	0	+2	+4	+3	+4	+3	+4	+1
EVENT 8	+2	+2	+1	+2	+5	+2	-1	+1	+1
EVENT 9	+5	+1	+4	+5	+2	0	+1	+2	+3

Using an example from this chart, if Event 1, the United Nations signs a treaty providing for the prosecution of world-wide cyber criminals, were to occur, then it would have a positive impact on Trend 1, the use of the Internet for commerce. Conversely, if Event 5, establishment of a Uniform User Identification Act, were to occur, then it would have a negative impact on Trend 7, public pressure over cyberfraud prosecution. Therefore, the information developed in this matrix concerning the cross impact analysis could, and should, be utilized to construct a strategic plan that will favorably affect the issue.

Using the cross-impact analysis (Table 5), Events 5, 6, 7 and 9, respectively the uniformed user identification act, limiting anonymous Internet use, biometric e-commerce use and an industry repository for reporting cyberfraud, can be used to impact favorably upon Trend 1, use of the Internet for commerce. Each of these events are rated at +5, and therefore will have a great positive impact on Internet commerce, which the group believes will in turn have a positive impact on the ability to prosecute interstate cyberfraud. Accordingly, the strategic plan should adopt measures that will be most favorable to causing these events to occur.

Event 3, the usage of high technology courtrooms, has the greatest positive impact on Trend 4, 5 and 8, Internet speed, prosecutorial resistance to handling cyberfraud cases and development of high technology courtrooms, all of which scored a +5. Therefore, designing a strategic plan, which will foster the occurrence of the development and implementation of high technology courtrooms, will favorably influence the ability to prosecute interstate cyberfraud.

Conversely, Event 2, the development of a national forensics network, will have very little positive impact, and actually a somewhat neutral impact on virtually every trend. Given this information, the strategic plan should not focus on generating situations which would cause Event 2 to occur, as this event has little benefit to the prosecution of interstate cyberfraud. In effect, by designing systems that take into account the cross impact analysis, the outcome of the future may be impacted. Using this information allows steering to take place, as opposed to rowing toward an uncertain destiny.²³

Alternative Scenarios

By analyzing the trends and events developed by the NGT process, and by studying the cross impact analysis, a vision of the future can be developed. The following three scenarios were developed regarding how interstate cyberfraud will be prosecuted in the future. The first scenario depicts an optimistic future and is based on the positive material developed via the NGT process. The events portrayed in this scenario should be encouraged in order to affect a positive impact on the future of prosecuting interstate cyberfraud. The second scenario depicts a pessimistic future and utilizes material developed by the NGT process that paints a bleaker image of the future of interstate cyberfraud prosecution. The events portrayed in this scenario should be discouraged. The third scenario is normative, meaning that it is surprise free, and that if events continue on their present path, *ceterus parabus*, that is all things being equal, we will have no surprises down the road concerning the prosecution of interstate cyberfraud.

Scenario One: Optimistic

It's April 24, 2004. Captain Sanchez leaned back in his ergonomically designed chair and studied the reports on the computer screen in his home study in Ojai, California. Now that the government has provided what amounts to unlimited funding to pursue cyberfraud, the captain had all the work he could handle. The multi-jurisdictional cyberfraud team consisted of ten eight-person squads. Each squad was equipped with a high technology van, a network engineer, and four cybersleuth certified investigators, and enough software and hardware to run a multi-national corporation.

Captain Sanchez watched on the screen as one of his squads raided a hacker's nest in Tennessee. The cyber crooks did not know what hit them, and therefore did not have an opportunity to scatter like the little cockroaches they appeared to imitate. Since the advent of real-time cyber transmissions, the evidence that was gathered was now instantly reviewed. As Sanchez watched the events unfold, so did an impaneled Grand Jury. By the end of the day, the operation would be finished, and an indictment would be issued.

The trial would be quick, as the legal wrangling to age the case was removed years ago by the passage of laws that allowed victims to testify using cybercourts in their own towns. No longer did victims have to travel to distant venues to seek justice. Cases were streamlined, and justice administered rapidly. Criminal sentences were imposed virtually immediately, and the roving bands of cyber predators were being rapidly reduced in virtually all areas across the nation.

Sanchez smiled at the prospect of next week's signing of the International Cyberterrorism Treaty. Sanchez's team was busy now, but their caseload was nothing compared to what it would become when they were allowed to stalk cyber criminals on an international scale. The institutions that generated hackers by the bushel in Manila were ripe for the picking. Sanchez relished the impending activity and the potential calm the future arrests would bring to the cyber community.

Scenario Two: Pessimistic

Officer O'Neal schlepped his gear out to his patrol hovercraft. Briefing had been another barrage of cyber-related criminal acts. He had listened about how a hacker had

brought down the city's power grid and caused a traffic collision that killed three motorists. The mayor was screaming for the department to arrest the suspect, but since the ACLU was successful in allowing all on-line identities to remain confidential, there was little chance of that happening. Everyone, it seemed to O'Neal, has a right to remain anonymous. With such impunity, why not loot and pillage to your heart's content?

When O'Neal factored in the recent scandal wherein five department administrators were arrested for running a runaway child Internet sex slave ring, he was disgusted. Ever since President Gore's Internet Czar mandated free computers and Internet access for all citizens two years ago, things have not been the same. The department was not prepared for the onslaught of new cases. Furthermore, the cybergoons tended to make sure they victimized folks who lived in other jurisdictions, making prosecution a virtual impossibility.

The FBI had promised to wage a war on the new generation of cyberfraud perpetrators when it received the funding to hire three thousand new agents. That promise had gone unfulfilled, as the agency was unable to lure technologically literate citizens to become agents. It seems federal law enforcement duty paid just above the poverty line, and being a methamphetamine addict with free computer access was simply more alluring.

O'Neal slung his gear into the hovercraft's back seat and buckled himself in for what promised to be a non-stop tour through cyberhell. O'Neal punched the ignition button on the craft. The dashboard LCD's lit up, but the engine failed to roar to life. A digital skull and crossbones materialized on the LCD display. The skull cackled as a neon red set of letters flashed, "GOT CHA!" at an infuriating pace. A computer voice

began chiming, “Warning. Wireless digital interface compromised.” Over and over the warning repeated. O’Neal would have to reboot his craft and hope that the emergency backup disk had not been compromised as well.

O’Neal sighed and slumped down further in his seat as he set about what would undoubtedly be a laborious task. He secretly wished he had paid closer attention to his computer coursework in college. Had he had more aptitude, he could have joined the Federal Cyber Coalition and been giving away computers to pay off his college debt. But, no, he chased women and drank his way through school, and was relegated to working off his loan by pushing a black and white around a city full of hackers bent on making his job as miserable as possible.

Scenario Three: Normative

Detective Johnson sat down at the computer terminal and began reading his e-mail. Johnson found it amazing that so many requests for investigation could be generated overnight. Ever since the department received the Office of Criminal Justice Planning (OCJP) grant for a cyberfraud investigation unit, Johnson had been swamped. Johnson was intrigued by computers and played on systems at home as a hobby. When the position for cybersleuth became available, the captain had offered him the position based on his aptitude with computers.

Next month, the OCJP grant was being increased, and another investigator would join the team. The new investigator would come from the adjoining jurisdiction, thus creating a true multi-jurisdictional task force. The MOU provided for the District Attorney’s Office to contribute a deputy DA to vertically prosecute the suspects Johnson

and his yet to be named partner captured. The work was tedious, but rewarding. Johnson always smiled inwardly when fellow detectives shook their heads in amazement at the cases he was able to successfully pursue to conclusion. Johnson's workstation was loaded with plaques from various organizations recognizing him for his dedication to investigating computer-related crime.

In his spare time, Johnson had been lobbying the state legislature to champion a bill giving law enforcement officers the ability to cross state lines to pursue and prosecute cyber criminals. Tomorrow he had an appointment with Senator Gomez to finalize the bill's wording. If all went well, the legislature could process the bill in about twelve months. Governor Sitting Bull promised to sign the bill when it made its way to his desk. Johnson could not wait to start chasing the Internet crooks into the dark lairs, where up until now they operated anonymously and with impunity across state lines.

Johnson, also the state High Technology Crime Investigation Association (HTCIA) president, opened a blank Word document and began to ponder the letter he was preparing to write. He wanted the letter to come across strong, but not threatening. If the President's Commission on Internet Literacy was successful, every citizen in the country would have access to a free computer and free Internet access as well. If that happened, ordinary criminals would take to cyberfraud like ducks to water. Once opened, the floodgates would be impossible to close. If the President was insistent on making everyone Internet savvy, then he would just have to provide the funding to increase cyber patrols. Johnson was committed to illuminating the situation sufficiently to ensure cyber criminals did not proliferate to the point of dominance. Johnson was committed to success, and he would not rest until his mission succeeded.

The information developed in this chapter demonstrates that several trends and potential events call for action by way of legislation that will enable the introduction of technology into courtroom environments and will facilitate the investigation of and prosecution of interstate cyberfraud. The next chapter will develop a strategic plan that can lead to the successful implementation of regulations and laws that will positively affect the future prosecution of interstate cyberfraud.

CHAPTER III

STRATEGIC PLAN

Introduction

The purpose of this chapter is to develop a strategic plan for the implementation of systems that will facilitate the prosecution of interstate cyberfraud. This strategic plan is based on Scenario One, the optimistic scenario. The literature and legal scholars evaluated for this project agree that developing a system that allows states to prosecute crimes that occur over interstate borders is going to be a legal minefield, requiring every state to adopt an agreement allowing for such prosecutions at the state level.

Alternatively, having a mired federal criminal justice system agree to investigate and prosecute every Internet-related crime occurring over state boundaries is overwhelming to the scarce resources of the federal government. Either direction requires travel over what, at first, appears to be an insurmountable minefield of legal issues, personnel issues, training issues and political issues.

Since this issue is currently upon society, law enforcement agencies must deal with it. Law enforcement professionals should have been tackling these issues years ago when they first realized the potential scope of the issues. Unfortunately, they did not do that. In traditional fashion with issues that are not fully comprehended, law enforcement turned a blind eye all the while chanting a mantra about how someone ought to address the issue. Law enforcement cannot address the issues that have already passed them by, but can and must make plans for the future. These plans must be acted upon so that law

enforcement officials can shape their own destiny, rather than have that fate thrust down their throats.

This chapter will examine the impact different influences could have on the issue. A discussion will follow this examination on how we can best mitigate the negative issues while exploiting the positive virtues in an attempt to plan for a desired future. The internal and external influences on the issue will be discussed, identifying weaknesses, opportunities, threats and strengths related to the issue. Additionally, relevant stakeholders and snaildarters (unanticipated obstacles) will be identified and examined.

Weaknesses

- Fear of the unknown often generates paralysis. If something is not understood, society is hesitant to embrace it. Law enforcement is not immune to fear of change.
- Additional laws will need to be established.
- There is a potential for feuding over funding between local, state and federal agencies.
- Law enforcement entities are frequently hesitant and suspicious as well as reluctant to work together cooperatively.
- There are serious legal issues involving prosecuting crimes that victimize individuals in one state, yet have their origin in another state. These crimes are traditionally seen as the purview of federal agencies.

Opportunities

- Increased ability to prosecute crimes that have traditionally gone unpunished.
- Ability to train a new generation of forward-thinking investigators in technology-related criminal investigations.
- The technology industry would embrace the opportunity to strengthen criminal deterrents and may well offer funding to create prosecution opportunities.
- Younger law enforcement officers and prosecutors entering the field frequently come armed with technological experience which would make training the next generation of cyber sleuths easier.
- Opportunities to track cyber criminals may generate renewed interest in law enforcement as a career path for college educated individuals with degrees in the computer field.
- High technology crime is on everyone's mind, and thus the opportunity to expand interest while attention is focused on the issue is great.

Threats

- There is a great potential for turf wars over federal agencies giving up ground on traditionally federal interstate venues to local investigation and prosecution.
- It will be difficult to rally every state to enact and sign legislation that forms the basis for an interstate compact to prosecute cybercrime.
- The ACLU and other interest groups will oppose the expanded powers such an initiative will create.

- Legal challenges may draw out the successful implementation of interstate prosecution for years.
- Federal agencies will have to relinquish some control over their ability to prosecute.

Strengths

- High technology crime investigators take enormous pride in their ability to track cyber criminals.
- American ingenuity has a history of overcoming seemingly insurmountable obstacles.
- New legislation would generate increased capacity for prosecuting high technology crime by using technology to reduce the expense of prosecuting.
- Criminals would no longer be able to act with impunity as they committed their crimes across state lines.

Stakeholders

Stakeholders are the people who have the opportunity to play a significant role in the outcome of an issue. Depending upon their actions, an issue can succeed or fail.

Stakeholders may influence outcomes or be influenced by others concerning the issue.

The people listed below are the individuals or groups whose involvement in the planning of the issue is necessary in order for the issue to meet with success:

- Elected Federal Officials. Elected federal officials are the representatives of the population. They have to balance the needs of the citizens against the rights of

- the citizens and the accused defendants. The federal officials must also determine how to budget the funds necessary to both protect and provide for society. Any legislation enabling interstate prosecution must receive congressional approval.
- Elected State Officials. Elected state officials are the representatives of the population. They have to balance the needs of the citizens against the rights of the citizens and the accused defendants. The state officials must also determine how to budget the funds necessary to both protect and provide for society. In order for any federal legislation enabling interstate enforcement of cyberfraud statutes to occur, state officials must be willing to cooperate with federal authorities.
 - Elected City and County Officials. City and County officials must be willing to fund law enforcement positions to deal with interstate cyberfraud statutes enacted by state and federal authorities. If the laws exist, but the positions to enforce the laws are not funded, then any statutes are effectively dead in the water for lack of interest. City and County officials must look into the future and make a decision regarding the import of such investments in person power, training and equipment.
 - Federal Bureau of Investigation. The FBI has traditionally been the agency tasked with investigating interstate crime. The FBI must be willing to let down its defenses and share a small portion of its jurisdiction in order to safeguard the public from the crimes that victimize them. By doing this, there is recourse for victims.

- Citizens of the United States. The public must become aware of the level of cyberfraud and the danger of allowing it to continue unchecked. The public has limitations to the amount of taxes they are willing to pay, and choices must be made in order to direct funding appropriately.
- Professional Associations. Many professional associations have a vested interest in interstate cyberfraud. CPA's, police officers, fraud investigators and others know what a valuable tool enhancing their ability to reach across state lines can be. Their resources can and should be harnessed in order to tap into their combined experience.
- Peace Officers. Increased training and expertise will be required to investigate interstate cyberfraud. Police officers should be encouraged to look at the benefits of investigating and prosecuting interstate fraud suspects.
- Criminal Defense Attorneys. Defense attorneys may not see the immediate benefit to expanding local law enforcement's ability to investigate and prosecute interstate cyberfraud. A conscientious effort will have to be made to encourage their cooperation and support for the necessary legislation.
- County, State and Federal Prosecutors. Many professionals exist in a comfort zone. Inside that zone, developing new difficult skills is often discouraged. Developing new laws to allow the prosecution of cyberfraud will force prosecutors to learn new skills in technology and fraud. With the proper approach, this transition can be made to appear appealing.
- State and Federal Judges. Case management and workflow are paramount to effectively managing a criminal docket. Increased case filings from the passage

of Interstate cyberfraud legislation may be seen as a daunting prospect. By explaining the benefits to society of such a program, judges may soften their view on the added workload that may be generated by such legislation.

Snaildarters

Snaildarters are stakeholders, events or processes that have not yet been identified, but which could become unanticipated obstacles to the issue. The following is a list of potential snaildarters:

- Civil Libertarians. The ALCU is all about protecting the rights of citizens. It routinely opposes legislation that expands traditional authority granted to any governmental entity.
- American Bar Association. The ABA and attorneys who are members tend to be liberal thinkers, and long on conservative approaches to innovation that may expose their clients to additional penalties. The ABA has a powerful lobby that can derail legislation or alter it to the point where it is ineffective.
- Federal Officials. Federal officials guard their territory jealously. Look for high-ranking officials to oppose any attempt to increase state rights, as must be done in order to expand the state's ability to investigate and prosecute interstate cyberfraud.

Strategies

Any large-scale operation requires a roadmap and a game plan. Without giving great quantity of thought to the goal and the development of the strategies to get

successfully to the end, any monumental operation is doomed to failure. Accordingly, the following strategies need to be considered in order to implement the ability to prosecute interstate cyberfraud:

A. Research. A team should be assembled representing each of the stakeholders.

By bringing the stakeholders into the fold, they have a say in how the final product is crafted, and in how things will actually work.

B. Identify.

1. Supporters. This is to be done through the research team, and will identify those groups and organizations who will provide support for the project.
2. Detractors. The research team will also identify groups and organizations that will oppose the goal of the team and will work to keep things status quo.
3. Issues. The research team will work with market analysts to determine external issues, and with government advisors to develop a list of internal issues that will affect the ability of the group to successfully complete their task.
4. Conflicts. Every effort must be made for the team to identify any internal or external conflicts that will cause the project to become sidetracked or derailed. Once identified, then solutions will be sought to overcome these potential conflicts.

- C. Perform outreach. Public hearings and presentations to various organizations, as well as press releases and interviews will have to be conducted to inform the public of the issues and the potential resolution to the problems identified.
- D. Extol the Virtues. After gathering public comment and determining opposition positions, a public relations campaign should be undertaken to inform the populace of the benefits of the proposed solution to interstate cyberfraud. In essence, inspire the masses.²⁴
- E. Determine costs. As part of the overall approach, costs must be determined and a plan to pay the expenses developed. Stakeholders and snaildarters must be carefully considered when developing this part of the strategy.
- F. Initiate legislation. The team will need to identify a legislator who will introduce the legislation and work closely with the elected officials to ensure passage of the appropriate laws.
- G. Develop a test case. After passage of the legislation, an appropriate test case should be solicited for investigation and prosecution. This case must have a high degree of probable success, with clear-cut issues in order to ensure success.
- H. Implement the program nationwide. Once the test case has been successfully completed, institute the program on a nationwide basis.

At present, there is no unified direction being pursued to address the issue of prosecuting interstate cyberfraud at the local, state, national or international level. The law enforcement community has to some degree addressed interstate cyberfraud at the

federal level, but that level of involvement does little to assuage the criminal deeds perpetrated against small business and residents that are quite literally not made into federal cases. By adopting this strategy, the law enforcement community can positively impact its ability to successfully prosecute criminals who commit interstate cyberfraud.

The information developed in this chapter demonstrates that effective planning can direct events that will lead to an increased probability that technology will be introduced into courtroom environments and thus facilitate the investigation of and prosecution of interstate cyberfraud. The next chapter will develop a transition management plan that can be utilized to successfully implement this strategic plan. The roadmap developed in the transition management plan is crucial to the ultimate development of regulations and laws that will positively affect the future prosecution of interstate cyberfraud.

CHAPTER IV

TRANSITION MANAGEMENT PLAN

Introduction

In order to successfully implement an interstate cyberfraud prosecution effort, a transition management plan is required, since only the federal government may presently successfully prosecute interstate cyberfraud. The transition management plan may be used as the process to implement the strategic plan.

Through the Nominal Group Technique process, in addition to reviewing literature and interviewing experts, it became obvious that although the ability to prosecute interstate cyberfraud at the state level is highly desirable, there will be many battles to be fought, with resistance met at many junctures. Accordingly, a transition management plan is necessary to provide a roadmap in this unfamiliar territory which will make the terrain as even as possible.

Stakeholders

In order to develop a transition management plan which will successfully enable law enforcement to prosecute interstate cyberfraud activity, certain stakeholders must provide active support to ensure success. These stakeholders, who have been previously discussed, have been identified as:

- Elected Federal Officials
- Elected State Officials
- Elected City and County Officials

- Federal Bureau of Investigation
- Citizens of the United States
- Professional Associations
- Peace Officers
- Criminal Defense Attorneys
- County, State and Federal Prosecutors
- State and Federal Judges

Plan Elements

A transition management plan cannot be finalized without buy-in from the aforementioned stakeholders, and effective mitigation of snaildarters. In order to ensure the successful development of such a plan, the requisites of the Transition Management Plan must include the following elements.

1. Develop an oversight committee. This oversight committee will need to be established to study every element of the Transition Management Plan and to recommend appropriate activities and strategies. This team will be composed of experts in cyberfraud, experts in computer technology, experts in constitutional law and experts in facilitating change. The team should be composed of county, state and federal prosecutors, local, state and federal law enforcement officials, business community members from high technology fields, and consumer advocates to represent the needs and concerns of consumers. Every member of the team needs to have a strong dedication to the success of the transition management plan.

2. Identify the present state of the issue. The oversight committee will investigate, define and prepare a written document that identifies the present state of the issue, including the positive and negative material that will either assist or inhibit future action regarding the prosecution of interstate cyberfraud.
3. Identify the future state of the issue. The oversight committee will seek expert advice from prosecutors, peace officers, convicted cyber criminals, stakeholders and snaildarters in order to identify the future state of prosecuting interstate cyberfraud.
4. Determine what changes need to be accomplished. Based on identifying the present state and future state of prosecuting interstate cyberfraud, the oversight committee will prepare a document detailing the changes that need to be accomplished, including the order in which they need to be accomplished and the importance to the overall success of the program of each item to be accomplished.
5. Facilitate an environment in which stakeholders are prepared to accept change. The oversight committee will prepare the requisite documentation for a plan designed to encourage support for the planned changes in order to positively influence the law enforcement's ability to prosecute cyberfraud with the support of the stakeholders that were identified. During this phase, relationships with legislators willing to sponsor required legislation need to be solidified, and their staff's input sought.

6. Develop a communication plan. Lastly, the oversight committee will develop a communication plan designed to spread the word about prosecuting interstate cyberfraud and the need for change. The communication plan will target all aspects of the groups who will be impacted by the changes, including the public, the computer industry, law enforcement, prosecutors, and elected state and federal officials.

The Importance of Planning

Whether a strategic plan and transition management plan exist, there is no guarantee that implementing a system to prosecute interstate cyberfraud will go smoothly or even happen at all. Having a strategic plan and transition management plan does, however, ensure that those involved in the planning effort are able to have a roadmap guiding our efforts, thus ensuring less chaos and more organization. As we learned as children reading Aesop's fabled ant and grasshopper story, planning efforts pay valuable dividends. Establishing leadership early on in the process will be fruitful and greatly assist the transition effort. Additionally, legislators, prosecutors, prosecutorial organizations, law enforcement organizations, high technology groups and trade organizations will all have to come together in consensus to develop a viable method by which to prosecute interstate cyberfraud. Such implications are discussed further in the next chapter.

CHAPTER V

IMPLICATIONS AND CONCLUSIONS

Introduction

It is imperative that the national implications of combating cyberfraud be brought to the public consciousness. Law enforcement officials have begun planning and implementing regional laboratories and teams of investigators to address high technology crime, however interstate cyberfraud is not presently being addressed, thus the criminals who engage in such activities continue to operate largely with impunity. A multifaceted approach is required to effectively combat this new wave of criminal activity that threatens to undermine our economy and the public trust in electronic commerce.

Every state in the country has local and state peace officers already assigned to address interstate cyberfraud, and therefore the most manageable and significant solution is at our fingertips: legislate interstate cyberfraud prosecutions by agreements between all of the states so as to allow county and state prosecutors to pursue cyberfraud across interstate lines. Absent a local ability to prosecute, a federal bureaucracy of epic proportions would be necessary to police interstate cyberfraud. Accordingly, a number of implications for influencing this issue call out to be addressed.

Leadership Implications

Implementing a plan to allow for the investigation and prosecution of interstate cyberfraud will have a national affect, calling for leadership at various levels of government and from different stakeholder organizations. In order to affect the smooth

development and implementation of a transition management plan, the leaders of these organizations must understand the intricacies of the issue and communicate it to their constituents effectively and supportively.

- Elected State and Federal Officials. These officials must demonstrate leadership to their constituents, their peers and their subordinates if successful development and implementation of a multifaceted approach to combating interstate cyberfraud is to be realized. Positive leaders should be cultivated from this group who can act as intermediaries with the oversight committee.
- Prosecutors. Elected prosecutors will need to utilize their collective lobbying efforts, as well as their friendships with legislators in order to convince lawmakers of the need for enhanced legislation to deal effectively with the very real threat of interstate cyberfraud.
- Prosecutorial Organizations. Local, state and national prosecutors' associations must inform their membership of the efforts of the oversight committee, and educate their membership regarding the need for such legislation. These organizations can call on their lobbyists to assist in convincing legislators to enact appropriate legislation to give prosecutors and law enforcement the tools to do their job and protect the public from cyber predators.
- Law Enforcement Organizations. Law enforcement's collective support of an issue is oftentimes a near guarantee of a successful campaign. The hallmark of such an effort is logic and reason. By pooling their resources, law enforcement organizations can inform and educate their membership, inform legislators of the import of their crusade, and impact positively upon the enactment of necessary

legislation that will enable the successful investigation and prosecution of interstate cyberfraud.

- **High Technology Groups.** These groups have many members and stakeholders. Their participation is vital to the successful generation of legislation that will enable the investigation and prosecution of interstate cyberfraud. By providing leadership in informing their members of the benefits of such legislation, pressure can be brought to bear on legislators and thus ensure successful laws are crafted to deal with the issue.
- **Trade Organizations.** High technology, electronic and telecommunication industry trade associations can provide leadership by informing their customers of the need for change and the potential threat to consumers if the problems are left unchecked. These groups can also exert pressure on legislators in order to facilitate prompt passage of appropriate legislation.

Budgetary Implications

To equip every county in the country with a cyber courtroom that is high definition video conferencing capable will cost billions of dollars. To purchase equipment, train and fund the salaries and overhead of a squad of cyber cops for every county in the nation will cost more billions than equipping the cyber courtrooms. Make no mistake, the ability to develop the infrastructure and purchase the equipment to investigate and prosecute interstate cyberfraud hangs on the oversight committee's ability to develop a stable funding mechanism. This funding must be from broad based sources, and must have minimal impact on governmental and consumer budgets. Industry will be

unwilling to pay additional taxes, and consumers will be very wary of advancing funds to the government for a service many believe should be provided without additional charge as a safety benefit to the public.

Developing a successful legislative package will be relatively simple in contrast to the designing of a comprehensive funding mechanism for interstate cyberfraud prosecution. Raiding existing special interest funds will be unsuccessful, and therefore, new sources of funding must be developed. Perhaps the easiest and least painful mechanism to employ is a national user tax for Internet service. Appropriate lobbying efforts, advertising and public relations will necessarily be the cornerstone of developing a sustainable revenue stream to fund these efforts. Much consideration must be given to developing a funding package, and operatives at the highest level will need to be involved in this process.

Evaluation Activities

The oversight committee will set benchmarks, and develop a Gant chart designed to identify critical completion dates for elements of the project. Target dates will be set and enforced to ensure forward momentum is developed and maintained. Surveys will be utilized in conjunction with press releases in order to ensure the message of the project is reaching the target audience of legislators, consumers, prosecutors and law enforcement officers. Routine evaluation will be critical to ensure the project remains on task and on its established timeline.

Recommendations

To adequately address interstate cyberfraud, a multi-pronged approach must be adopted. Fastidious attention to both the big picture and the details must occur in order to interweave a viable product that will be consumed without remorse. This approach should include:

- Adapting the Interstate Witness Compact to allow for out of state witnesses to testify via high definition video conferencing systems from court facilities that are in close proximity to their home or office. This will make the cost of prosecuting interstate cyberfraud much more reasonable and will pave the way to use similar testimony in other arenas after the system have proven its value.
- Establishing a system of cross-designation for law enforcement authorities assigned to investigate interstate cyberfraud. This will allow for officials to have the legal authority to investigate and enforce cyber crimes that cross state lines. Such cross-designation will require new laws at the state and federal level.
- Training law enforcement officials and establishing true multi-jurisdictional task forces to address the increasing threat of interstate cyberfraud. Local, state and federal law enforcement officers, as well as computer professionals will populate these task forces. Technicians who have a firm grasp on present and future technology will also be utilized.

Conclusion

Although cyberfraud activities are relatively new, any analysis that is done by a layman will quickly identify that cyberfraud is really nothing more than a high tech con game. Criminals have come of age and learned to use technology to separate generally innocent victims from their legitimate earnings. Face-to-face meetings are no longer required in order to engender trust between a con man and his target. Close proximity is also no longer a variable in this criminal equation.

Law enforcement agencies must act quickly before the game is over and the interstate cyberfraud swindles so pervasive that the proverbial barn door is incapable of being closed. Technology has erased geopolitical boundaries, however our laws have failed to keep pace. Only fast acting leadership will be able to close the gap created and exploited by cyber criminals.

Law enforcement does not traditionally hire computer experts, nor does the average peace officer or detective consider fraud a meat and potatoes type of criminal activity. Law enforcement is also traditionally unwilling to share information or glory (successes) with other local, state or federal agencies. In the world of cyberfraud, beliefs, hiring practices and close-mindedness collide with disastrous consequences. In order to successfully combat and prosecute cyberfraud, law enforcement officials must pull together, put their differences aside, and commit to working together as a team dedicated toward successfully implementing a cohesive, inclusive plan that effectively targets cyber criminals. Such synergy is imperative to success.²⁵

Though not a panacea, development of the ability to prosecute interstate cyberfraud will lead to the next logical step of prosecuting international cyberfraud. Law

enforcement has the ability to address interstate cyberfraud now. The technology and training is available, and long-term funding can be secured. If law enforcement fails to act, to become captains of its own cyber destiny, then law enforcement will no doubt one day become slaves to cyber terrorism by virtue of its own inaction. Law enforcement can be proactive, or reactive. Law enforcement leaders can wait for someone else to take up the charge, or they can set about to change the world. These plans must be acted upon so that law enforcement officials can shape providence, rather than have a probable dismal destiny thrust down their throats.

Left to our own devices and absent willing leadership, interstate cyberfraud prosecution capabilities for local and state agencies will remain a dream. A team approach to tackling the issue of interstate cyberfraud prosecution is required, and representatives from local, state and national law enforcement agencies are mandatory committee members for any oversight team responsible for development and implementation of this plan. Individual state or local agencies lack the capacity to ramrod an operation of such scope. The implications of developing the ability to prosecute interstate cyberfraud is such a potential logistical nightmare, only a very large organization with access to incredible resources and manpower pools has the opportunity to successfully develop and implement the plan presented here.

One organization meets the size and interest requirements necessary to undertake such a mammoth operation. The International Association of Chief's of Police (IACP) represents thousands of police administrators in every region of the country, as well as virtually every nation in the world. IACP is a logical organization to look to for the leadership necessary to establishing a credible voice at all levels, as well as an

organization with international membership, which will thus ensure such an undertaking to develop the real ability to prosecute interstate cyberfraud at local and state levels is given the credibility it requires to succeed.

Appendix A

Nominal Group Technique Panel

Mr. Ross Strowig

Special Agent, Federal Bureau of Investigation

White Collar Crime Investigations and former county prosecutor

Deputy Attorney General Jim Root

California Attorney General's Office, High Technology Crime Unit

High Technology Crime Prosecutor & Advisor to Regional High Tech Crime Teams

Mr. James B. Hackleman

Chief Deputy District Attorney, San Bernardino County District Attorney's Office

High Technology Crime Prosecution Policy Advisor

Mr. Brian Moore

Supervising District Attorney's Investigator, San Bernardino County District Attorney's Office

Investigating Member of San Bernardino County High Technology Crime Unit

Mr. Clete Hyman

Deputy Chief, Redlands Police Department

Commanding Officer of San Bernardino County High Technology Crime Unit

Mr. Kris Wandro

Computer Network Services Supervisor, San Bernardino County District Attorney's Office

Supervisor of Information Services and Network Technology for DA's Office

Appendix B

List of Trends

1. Offenses that occur in multiple jurisdictions.
2. Use of Internet for Commerce.
3. Electronic funds transfers (EFT) . Biometric based.
4. Russian Organized Crime Influence.
5. Computers with greatly enhanced capabilities.
6. Speed of Internet.
7. Video Conferencing.
8. Coordination between state, federal and local authorities.
9. Implementation of multi-agency task forces.
10. Wireless based communications.
11. Economic conditions.
12. Disgruntled employees.
13. Resistance by local prosecutors to handle cyber crime.
14. Fingerprint ID used in commerce.
15. Suspicion of government monitoring (big brother).
16. Public awareness of Internet fraud.
17. Keeping pace with Technology when training personnel.
18. Public Awareness/understanding of technology.
19. Federal cyber crime task forces.
20. Nationwide forensic networking.

21. Coordination between LE and private industry.
22. Federal and State funding for Internet crime units.
23. Reciprocal agreements between states (IE PC 1334).
24. Specialization Syndrome.
25. Computer security systems.
26. Knowledge/awareness by LE of cyber crime.
27. Use of computers as communication device.
28. State recognizing Peace Officer powers in alternate states.
29. Global Internet utilization.
30. Use of virus in communication interruption.
31. Computer SDT's (Subpoena Duces Tecum).
32. Local responsibility? Local jurisdiction?
33. Problems with obtaining records (interstate).
34. Conflicting "privacy standards" between states.
35. Business cooperation with disclosure.
36. Obsolete laws and wording in laws.
37. Ability to retrieve information (achieving).
38. Public pressure for enforcement of cyber crimes.
39. Obtaining user consent prior to use (Privacy Consent Waivers for Internet).
40. Use of escrow accounts.
41. Availability of personal and public information on Internet (auto-track).
42. Federal funding for local prosecution of cyber crime.
43. On line consultations with experts in fields of interest.

44. Use of Internet for teleconferencing.
45. Federal 790 statute allowing for cyber crimes in multi- jurisdictions to be handled
by one federal or state location (erasing boundaries).
46. Pirating software (music, Napster).
47. High tech use for teleconferencing.
48. Electronic High Tech Courtroom.
49. Anonymous activity on the Net.
50. Organized Crime use of the Net.
51. Identity theft.

Appendix C

List of Events

1. Development of a national forensics network.
2. Cross designation of law enforcement officers between states.
3. Internet II is open to public.
4. Teenager hacks into computer and opens Dam spillway control.
5. Uniformed User Identification Act.
6. Federal Interstate small claims act passed.
7. Laws eliminating anon use of Internet.
8. Limits placed on encryption.
9. Major cyber terrorist act.
10. World wide monetary system established (In Seattle).
11. Defendant clearing house for cyber criminals.
12. President Bush victim of ID theft.
13. High Tech Court rooms become acceptable.
14. Expand penal code 1524 .2 to allow in state officers to issue subpoena for bank records.
15. Laws passed to require computer record achieving.
16. Subject arrested for distributing bogus Bloomberg report.
17. FBI establishes cyber unit.
18. Tougher Laws for hacking.
19. Central database established for private industry reports for cyberfraud.

20. Permanent IP address or identifying number to individuals.
21. E-Bay Auction site shut down.
22. New Federal Agency to deal with Cyberfraud.
23. NET Czar.
24. Biometric used for e-commerce.
25. CA Supreme requires computer forensics within 15 days of warrant.
26. UN signs international treaty to allow for prosecution of cyber criminals.
27. Nationwide paperless filing system (way out there).
28. FBI develops on line computer investigator (with shiny black shoes).
29. CA passes law to allow victims to testify internationally.
30. Anti-internet population in Dakota's exploding (anti-cyber clans).

Endnotes

-
- ¹ Encarta Encyclopedia on-line [<http://encarta.msn.com>], accessed June 12, 2001.
 - ² Ibid.
 - ³ Encarta Encyclopedia on-line [<http://encarta.msn.com>], accessed June 12, 2001.
 - ⁴ Encarta Encyclopedia on-line [<http://dictionary.msn.com>], accessed June 14, 2001.
 - ⁵ Rosenblatt, Kenneth S. "High Technology Crime", KSK Publications, San Jose, California. 1991.
 - ⁶ Ibid, pp. 3-4.
 - ⁷ Frank, Mari and Givens, Beth. Privacy Privacy!, Office Depot Publishing, Spring 1999, p. 3.
 - ⁸ James B. Hackleman interview, 2001.
 - ⁹ Ibid.
 - ¹⁰ Clete Hyman Interview, 2001.
 - ¹¹ Ibid.
 - ¹² Dennis L. Stout interview, 2001.
 - ¹³ Ibid.
 - ¹⁴ California Penal Code § 13848.
 - ¹⁵ Robert Morgester Interview, 1998.
 - ¹⁶ California Penal Code § 865.
 - ¹⁷ California Penal Code § 866.
 - ¹⁸ California Penal Code § 881.
 - ¹⁹ California Penal Code § 1334.
 - ²⁰ California Penal Code § 1347.
 - ²¹ James B. Hackleman interview, 2001 & Robert Morgester Interview, 1998.
 - ²² Encarta Encyclopedia on-line [<http://encarta.msn.com/>], accessed June 5, 2001.
 - ²³ Osborne, David and Gaebler, Ted. Reinventing Government, Plume Publishing, 1993, pp. 219-221.
 - ²⁴ Phillips, Donald T. Founding Fathers on Leadership, Warner Books, 1997, pp. 57-59.
 - ²⁵ Covey, Stephen R. Principle-Centered Leadership, Simon & Schuster, 1991, p. 46.

Bibliography

- California Penal Code, 2001 version. New York, NY. Lexis Publishing.
- Covey, Stephen R. 1991. Principle-Centered Leadership. New York, NY. Simon & Schuster, Inc.
- Frank, Mari and Givens, Beth. 1999. Privacy Privacy!. Office Depot Publishing.
- Hackleman, James B. Personal interview. San Bernardino, California. May 9, 2001.
- Hyman, Cletus. Personal interview. San Bernardino, California. April 13, 2001.
- Morgester, Robert. Personal interview. Sacramento, California. April 12, 1999.
- Morgester, Robert. Personal interview. Sacramento, California. March 16, 2001.
- Osborne, David and Gaebler, Ted. 1993. Reinventing Government. New York, New York. Plume Publishing.
- Phillips, Donald T. 1997. The Founding Fathers on Leadership. New York, NY. Time Warner, Inc.
- Rosenblatt, Kenneth S. 1991. High Technology Crime. San Jose, California. KSK Publications.
- Stout, Dennis L. Personal interview. San Bernardino, California. April 11, 2001.