

**THE FUTURE OF COMPUTER CRIME  
AND  
LAW ENFORCEMENT**

**BY**

**LYNN E. BUTTON  
COMMAND COLLEGE CLASS XVI  
PEACE OFFICER STANDARDS AND TRAINING (POST)**

**SACRAMENTO, CALIFORNIA  
JUNE 1993**

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

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

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

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

The attached article was written by a graduate of the Command College, Peace Officer Standards and Training (POST), California.

Technical details, information sources, and data analyses are contained in a separate report that may be obtained by submitting a request to:

The Center for Leadership Development  
Peace Officer Standards and Training (POST)  
1601 Alhambra Blvd.  
Sacramento, CA 95816-7083

Phone: (916) 739-2093

Please be sure to provide the name of the author.

## INTRODUCTION

The exploits of individuals using a computer for unlawful activity have graced media reporting over the past decade. The impact of computer crime on a large law enforcement agency by the year 2002 may be an issue of concern for the next decade. Also, other areas of concern for the next decade and which relate to the aforementioned issue are: will law enforcement have the responsibility for investigating computer crime; what type of training and education will be needed by the investigating body; and how will the investigating unit keep pace with technological advancements. Consider the following:

A man filed phony electronic refund claims with the IRS by using social security numbers from people who normally did not file claims. He was able to obtain speedy refund loans from banks with checks averaging \$3,000 and a net tally of nearly \$1 million. The IRS has been victimized by phony electronic refund thefts since they began offering electronic tax filing in 1986. In 1992, \$17.6 million in phony electronic fund claims was paid to computer scan artists.<sup>1</sup>

A hacker charged 11,733 telephone calls costing \$1,600 during August of 1992 to an emergency telephone located along a major freeway.<sup>2</sup>

Two teenagers broke into a computerized voice mail system, changed the company greeting to lewd messages, placed bomb threats, and erased customer messages and orders. The cost to the company was \$2.4 million. Stated reason: the teens did not receive a free promotional poster from Computerworld.<sup>3</sup>

A teenage son spent hours over a computer keyboard playing games and communicating with friends. All was fine until a Garden Grove telephone company greeted the father with a lawsuit, accusing his son of hacking long-distance lines to the tune of \$80,000. Thrifty Tel Inc. of Garden Grove estimates losses of \$22,000 a month due to such activities and telephone fraud is responsible for losses of \$5 billion a year or more. Giving kids a computer and a modem is like giving them a loaded gun. <sup>4</sup>

The aforementioned cases have occurred in today's world. Headlines in the future could include the following:

"Computer Smut King Goes Free." The United States Supreme Court reversed the decision of a 23 year-old computer pornography distributor who was involved in the shooting of a suspected gang member. The decision was based on an unlawful search and seizure by a computer investigation firm. Local law enforcement, not having the expertise to investigate the offense, received the go-ahead from City officials to contract with the firm. The firm, consisting of retired police officers with investigative experience, apprehended the suspect after monitoring an underground computer bulletin board. The court ruled that the firm was an extension of the police effort, acting as their agents and susceptible to the constitutional guarantees of search and seizure. Law enforcement officials reiterated the need for government-created ethical standards. Some headway was gained by law enforcement when two years after the homicide, legislation was enacted to establish security efforts and standards for computer users.

"Search and Seizure at the Forefront of Rambo Computer User." A computer hacker who caused the activation of a sophisticated military defense system was freed

from custody when the judge ruled that the police did not follow proper search and seizure protocol in accordance with the U. S. Constitution. The case has caused local government officials to contract with private firms specializing in computer crime investigation. "Law enforcement has been slow to react to this problem," was the cry from government officials. Police officials cited lack of funding, concern for ethics associated with computer usage and standards, too many vendors and operating systems, and inadequate security measures as the reason for their inability to fully and successfully investigate computer crime offenses. Law enforcement officials were also somewhat ambivalent regarding the decision due to the fact that they felt slighted by the lack of funding and support. However, they were relieved that the crimes will at best be investigated.

"Computer Group Marches on Capitol". A united group of computer enthusiasts called "Keep Data Free" marched on the Capitol in Sacramento, protesting their right to privacy and their dissent upon being referred to as "hackers." The group has contended that information transferred over electronic lines is open for public review, regardless of its ending destination. The group was ecstatic when the Federal Court of Appeals overturned the arrest of a 17 year-old boy who had altered credit history from a national data collection service. In the case, officers investigating the offense had been operating for one year when the case was uncovered; however, they did not obtain a search warrant for the arrest and seizure of the youth's computer system. The judge had received pressure from computer enthusiasts to ensure law enforcement complies with constitutional guarantees.

There are driving forces today which will cause the proliferation of computer crime into the future, greatly eclipsing present occurrences. The driving forces; namely, technology, information, computer technology and law enforcement, family shifts, hackers, and law enforcement involvement will lead to a different future outlook in ten years.

### Technology

Technological advancement can cause major shifts in society. As an example, a century ago 42.6 percent of Americans were farmers; whereas today less than 3 percent are farming. The use of chemicals, better seed, improved farming techniques and advancements in mechanization are the reasons for the change.<sup>5</sup>

There are a wide range of technological advances planned for the future. For example, technological advances for the automobile include the following: (1) radar/sonar, collision avoidance [1994], (2) in-dash navigation system [1995], (3) complete heads-up windshield display [1995], (4) rear seat and door-mounted air bags [1996], and (5) in-car parking structure reservations [1998].<sup>6</sup>

For the home of the future, high-tech toilets, automatic window controls, and motorized security cameras are slated<sup>7</sup> and personal computers will have the ability to recognize human voices in the not-so-distant future.<sup>8</sup> Telephones will be carried in the pocket which will allow one to identify callers and the nature of the call from any location.<sup>9</sup>

Technology will continue to allow for the office to be portable. Notebook computers, fax modems, portable printers, cellular phones, satellite linked pagers, etc., currently make this possible.<sup>10</sup>

Edward Cornish, a noted futurist, states that some of the important issues for the 90's will revolve around a shortage of energy.<sup>11</sup> Mr. Charles Taylor of the Army Corporation of Engineers supports the energy shortage theory and believes that there will be a new order of nations by 2010, as industrial nations will need energy. Thus, energy will become a valuable commodity and computer hackers will focus their attention on the confiscation of energy.<sup>12</sup>

An information "superhighway" connected by fiber optic cable will join scientists, students, educators, business people, citizens and others. The superhighway will virtually allow everyone the ability to communicate and access any number of information sources.<sup>13</sup>

Expert systems, artificial intelligence, neural networking, virtual reality, parallel processing, and robotics are some of the budding technologies which have the computer as their brain center. The advancement of these areas will provide society with quicker, cheaper, and more efficient ways of performing tasks and experience pleasure.

### Information

Information will be a driving force in the upcoming decades; and those who can create, process, and network will be the most successful.<sup>14</sup>

Information databases can reveal the name of a person, the social security number, address, and spouse's name, among other data. All such data can be accessible from home by a knowledgeable PC user.

Computer networking will take privacy loss a step further. The history of people will be on a single database and will be accessible by all.<sup>15</sup>

### Computer Technology and Law Enforcement

The growth of computer technology will be explained from two perspectives; one perspective rests with government's ability to keep pace with information/computer advancements, and the second perspective rests with the criminal element and their behavior.

#### The Government's Role in Technological Advancement

National, state and local governments have come to rely on computers. Lack of resources has forced government to look for efficient and economic ways to accomplish tasks. Computers are often installed because 80-85 percent of general fund budgets are consumed by personnel costs. Consequently, entities shave dollars through automation.

#### The Criminal Element

The more formidable of the two perspectives affecting law enforcement involves the criminal element. The average computer theft is between \$475,000 and \$560,000. It is no wonder that devious minds are attracted to this type of criminal activity. Compare this figure to an average of \$19,000 taken in a bank robbery.<sup>16</sup> A tremendous amount of time, effort, and publicity is spent capturing bank robbers and the electronic thief is being ignored. The sale of stolen goods, prostitution and pornography schemes, frauds,

thefts, and vandalism (viruses) to our computer systems are costing the taxpayers dearly.

Estimates show that computer criminals in the workplace alone may be costing business up to \$3 billion per year.<sup>17</sup> Reported computer and telecommunications crime losses amount to \$555 million per year, with unreported losses estimated at \$5 billion annually.<sup>18</sup> The FCC cites nearly \$500 million in fraudulent calls are placed through corporate PBX's each year.<sup>19</sup>

#### The Family Shift

Children today are exposed to and use electronic gadgets such as telephones, VCR's, video cameras, and computers with a variety of applications such as Spell Check and Grammar Correction. Middle-class children are conducting business with microchip products which can be purchased from department stores such as Sears, Wards, Macy's and other retail outlets. As a result, there is little interaction among family members. Interaction is occurring between children and their friends in bedrooms via computer modem. Thus the biological family has been supplanted by the electronic family. Today, 72 percent of households have video recorders, 78 percent have microwaves, and nearly 50 percent have computers at home or have access at school, up from less than a third in 1984.<sup>20</sup>

The National Institute of Justice sponsored three studies on the topic of computer crime. One conclusion reported computer criminals obtaining their skills at a very early age, usually from school. The children usually start by copying software and transcend to

credit card fraud. Their beliefs and information stem from contacts with other hackers.<sup>21</sup>

### The Hacker

The hacker believes that information is for all to access, and the issue of privacy will continue to surface in the future. The privacy question will have a bearing on information storage and access. Cyberpunks, who communicate with each other through electronic bulletin boards, are computer cowboys in a world of bitstreams and databases inside computer networks. With the tap of a key, they claim they could effectively cripple the economy or shut down communications systems the world over. If this is true, then Cyberpunks would become a formidable foe.<sup>22</sup>

### Law Enforcement's Involvement

A drug dealer can purchase a computer and via an electronic mail hookup, conduct illicit drug marketing. The reason this is possible is twofold: (1) computer system hardware and software is affordable, and (2) computer literacy among criminals is increasing. Criminals are moving beyond cellular phones and digital pagers to computer systems.<sup>23</sup>

Law enforcement is the logical entity to address such abuse; however, their position remains tenuous at best. Computer crime is esoteric and does not fit the mold of traditional crimes such as burglary or assault. Many law enforcement officers don't understand it, and because it doesn't involve physical danger to anyone it's likely to receive low priority treatment when it comes to investigations and prosecution.<sup>24</sup>

Unfortunately, the criminal justice system is slow to act and law enforcement has trouble keeping pace with technology. The police are preoccupied with traditional crimes such as robbery and burglary. The public is also preoccupied with these types of crimes. Thus, economic crimes, due to their low visibility, do not receive a priority response.<sup>25</sup>

Based on a 1990 survey, 72 percent of police and 88 percent of sheriffs and prosecutors do not have an individual unit that specializes in computer crime.<sup>26</sup>

As previously discussed, the availability of a computer, size, speed, power, and ease of use are being thrust upon society in rapid succession. The public will make the transition and move forward with new-found technology. If law enforcement does not adjust, it may suffer the consequences from a criminal subculture which continues to use available technologies to commit criminal offenses. The criminal who uses a computer to perpetrate offenses has increased potential to be very destructive. Therefore, the question for this article is what impact will computer crimes have on a large law enforcement agency over the next ten years? Other areas of concern are: Will the responsibility for investigating computer crimes rest with law enforcement? What type of training and education will be needed by the investigating body? How will the investigating unit keep pace with technology?

Shrinking revenues, budget cuts, and lack of computer expertise may be some of the reasons to question law enforcement's ability to investigate computer crimes. Conversely, there is a sense of duty to protect all citizens from the criminal elements, and law enforcement historically devotes resources to this task.

Training and education will be a concern for any unit investigating computer crime. The complexity and diversity of computer crime offenses makes them different than traditional law enforcement criminal investigations. The need to educate and train investigators, first responders, and management on this type of crime will be necessary.

Technology is changing at a seemingly exponential rate. New developments for electronic circuitry are shrinking the size of computers and making them more powerful. The concern for the investigating agency will be whether their budget will allow for the updating and or upgrading of equipment and training.

#### **THE FUTURE STATE**

The availability of information, level of security development and standards for computer systems, acceptance of shared ethics for computer use, the use of electronic fund transfer, and the level of funding to investigate computer crime violations are five trends worthy of concern over the next ten years.

Events which have a high probability of occurring include a judge ruling a violation of the Fourth Amendment for search and seizure, a hacker initiating a major military movement, sophisticated criminals forming an organization, police agencies contracting computer crimes investigations, and the death of a hospital patient.

It is believed that the availability of information will increase three-fold, security standards will double, ethics will change slightly, electronic fund transfers will triple in number, and funding of investigations will double over the next ten years. Information should not be as available due to privacy issues and law enforcement's inability to recognize computer crime as a threat. Ethics for computer use will be fraught with legal

challenges as to privacy. A lack of faith in law enforcement's ability in keep pace with technology and recognition that criminals will use high tech components for illicit activities will continue to be a concern. Thus, as electronic fund transfer becomes the norm, law enforcement will be expected to address theft incidents. As humanity approaches a moneyless society, electronic fund transfer will be used to purchase goods and services. Funding for investigating computer crimes will depend on the availability of money and whether high profile events bring forth attention and support.

The preceding engendered negative consequences from hampering law enforcement's ability to investigate computer crime in a timely manner to businesses and human lives suffering tragic ends. The three short future stories mentioned in the beginning of the introduction incorporated all of the aforementioned trends and events. One can readily see that the results are not desirable. The stories demonstrate how criminals using computers can cause severe repercussions and hinder investigations. Again, confidence in the police to investigate the crime and governments supporting role are the key elements.

### **PROBLEM APPROACH**

An agency desiring to impact the emergence of computer crime and mitigate an unwanted future state must recognize in its mission statement that these types of offenses are a priority. The mission statement describes areas where resources will be directed.

Once the mission statement is determined or modified and policies are generated, the development of a strategy must occur. There must be a requisite for sound planning in deciding the most effective strategy and its implementation transition.

Developing a strategy for implementation must include an appraisal of the internal capability of the organization and external influences which can impact the success rate. Identification of people or groups who can assist or hamper the strategy is paramount. In other words, a bit of troubleshooting before the development of the strategy increases the chance of success.

Different approaches, with the goal being development of strategies, should involve exploration of possible ideas from those involved. The ultimate identification of a key strategy, as well as possible alternatives, is essential to addressing a problem requiring a solution.

Below are examples of strategies which could impact the problem of computer crime in the future:

1. Emphasis on the need for state legislation which would allow law enforcement agencies to seize assets obtained by computer criminals. Such legislation, likened to the Narcotic Asset Forfeiture Statute, would require support from city and state officials as well as law enforcement agency heads.
2. Identification of the need for a specialized unit spread across the criminal justice system to identify, investigate, and prosecute computer criminals.
3. The modification of existing law by specifying that the use of a computer for the purpose of unlawful gain or for destruction is sufficient to establish criminal intent.

An evaluation as to the strengths, weaknesses, and level of support by persons or groups who can influence the key strategy is important prior to determining the final strategy selection. The establishment of a specialized unit, Strategy Example No. 2, is

the method which can impact the issue. An aggressive enforcement approach from three divisions of the criminal justice system would seem to be the best approach in countering the trends and events described in the three short stories. Also, the criminal justice system seems to function more efficiently when a shared concern allows for the participation of law enforcement, prosecution, and judiciary bodies.

Creating solutions to solve problems is an important step in altering the course of events or in obtaining a desired result. It is the implementation of the strategy or it's transition which seems most difficult. The remainder of this paper will delineate a planned implementation of the establishment of a computer crime unit, which is the selected strategy.

#### **EXAMPLE OF A PLANNED IMPLEMENTATION**

It is common knowledge that the disruption of one's comfort zone can lead to resistance to change. For purposes of plan implementation, a model agency will be used as the example for implementing the strategy. The Fresno Police Department will be the model agency of choice.

The City of Fresno is the largest city in the San Joaquin Valley and is located in the central region of California. The city is approximately 100 square miles and has a culturally diverse population of approximately 370,000. The Fresno Police Department has 650 employees of which 426 are sworn peace officers.

A key element in minimizing change is to identify groups or individuals who can cause the change to occur as smoothly and expeditiously as possible; conversely

identifying those who can cause the change to fail. The key people for the issue at hand could be:

1. Fresno Chief of Police
2. Fresno City Council
3. Fresno District Attorney
4. Telecommunication companies
5. Chamber of Commerce

### Management Structure

The Chief of Police, although the lead person for this project, does not have the technical expertise required for the strategy. He therefore must appoint a manager to facilitate the effective establishment of the computer crime investigation unit. The manager must work closely with the District Attorney's office and judicial unit to accomplish the strategy implementation. The Chief of Police must lend his support to the project and be willing to share the responsibility with those in charge of the other two government criminal justice agencies to encourage a joint approach.

The manager must have a solid technical base in understanding computers, and must possess good organizational skills, particularly with the two other criminal justice agencies. The manager must have strong interpersonal skills and be able to amicably interact with the lead members from the District Attorney's Office and the judicial representative. The manager must be able to share in the development of the program and coordinate its implementation. He must have the ability to interrelate with the City

Council, Board of Supervisors, and business community as an educator and information provider.

The Chief of Police would appoint a lieutenant to this position, expecting to be kept abreast of the progress of the project and planning of the transition. The Chief of Police would recognize that the manager must be empowered to ensure the implementation plan is enacted, especially with the other agency counterparts.

The manager must share responsibility with the representatives from the other criminal justice agencies. The manager would absorb the lead role on this committee since he possesses the technical expertise regarding computer crime. This shared committee approach would be expanded eventually to include members from the telecommunications companies and members from the business community.

#### Technologies and Methods

Change can be enigmatic if there is no manner or method to ease its inception. People are always affected when change is imminent; and if a comfort zone is disturbed, the change meets with resistance. The role of the manager is designed to take these factors into account and move the desired future state to reality. It is critical that the change be planned and organized and that information be given to all parties affected. The manager, in concert with the assistance of key people and others, can accommodate the change through time.

The key to change is to emphasize its positive attributes and diminish any negative energy which would hamper its success. For this reason, different techniques and

methods are used to heighten awareness and create a smooth transition. The methods and techniques to be used for this change would be the following:

#### Communication of the Vision

The desired future state must be clear and understandable. The vision must be understood by all affected parties. An articulation of what the change will accomplish is necessary and all involved parties must understand what the future will entail.

The Chief of Police must confirm the vision and the manager must communicate the vision to all parties. The vision statement should be written and understood by all. The manager should also meet personally with all affected parties to verbally communicate the points of the vision and eliminate confusion as to interpretation of the written document. The personal contact, whether by individual or group meetings, can also invoke instant feedback.

#### Role Model

Nothing detracts from a project or idea faster than negative energy. The manager must display an enthusiastic attitude, emphasizing positive movement. Any display of negative comments or feelings must be dealt with immediately. This can be accomplished through frequent meetings where information is exchanged, involvement of affected parties in decision-making, and celebration of small successes. Neglect in this area can cause discontent or frustration which hampers progress.

The fact that three criminal justice agencies would be involved in this project suggests that responsibilities need to be clear-cut so as to avoid duplication of effort and ensure accountability. The implementation team, consisting of the manager and

representatives from the District Attorney's Office and Judicial Office, need to generate a list of tasks which will lead to the success of the change. Once tasks are assigned, it is the members' responsibility to ensure success of the tasks. It is incumbent upon the manager to coordinate this effort and ensure, through weekly meetings, that progress is being made on each task. This would also allow for adjustments in task accomplishment.

#### Computer Crime Project Team

The three law enforcement agencies must educate themselves and work in tandem in order for the computer crime project team to come to fruition. After responsibilities have been determined and the manager and implementation members are more comfortable with each other, the implementation team should be expanded to include the business community and telecommunications companies. Selection of the business community members and telecommunications representatives should be made by the Chief of Police, the manager, the District Attorney's office, and the judiciary. The support of the additions to the transition team in the political process will be needed to overcome budget resistance from the City Council and Board of Supervisors. They can also augment the project with their involvement in training of the team members and assist in the procurement of state of the art equipment. The team should meet monthly to discuss progress. Lastly, prudent use of political influence could minimize budget resistance.

#### Goal-Setting and Time Management

A vision sets forth a desired result where one wants to be in the future. Once a desire is communicated, a plan and goals are soon to follow. The energy created by the

vision must be reached in an organized and timely fashion. Frustration is eliminated by allowing all parties to understand the needs and the direction required to reach the desired result. The manager will need to coordinate the activities of the project and assure that goals are established.

Time is a critical element during the implementation state. Individuals can become frustrated if they lose sight of the goals and spend their time performing tasks not related to the transition. Today's climate suggests that more work is being done with less people. A drawback to this type of thinking is that when people are given more work than time, tasks will be missed, unfinished or poorly performed. The manager must keep the focus on the transition and specify time lines, such as the use of a Gantt chart, to help keep track of the progress of the change. This will inform those involved with the change of the direction and time in which it should be accomplished.

### Rewards

Successes should be celebrated: everyone enjoys being told that they have done a good job. People are generally motivated when they are recognized for their efforts. The manager must ensure that individuals or groups receive recognition for their accomplishments. This can be done by formally acknowledging accomplishments in meetings, Council and Board of Supervisors proclamations, social outings for the implementation team, and something as simple as praising performance at the time of the accomplishment. These experiences promote positive energy and tend to reduce friction and frustration.

### Summary

Change can occur smoothly or can be erratic and destined for failure. Successful change is always the desired state. Once a vision has been created and a decision has been made to pursue the vision, a plan is developed to implement the change. The appointment of a manager to manage the implementation is a step to ensure the change is reached. Change is inevitable and people fear the effects of disturbing comfort levels when there is no clear communication. The manager can allay such fears with an organized plan for the change and through the use of interpersonal and management skills.

Computer crime invades privacy, is costly to the community, and can lead to tragic occurrences. The establishment of a computer crime investigation unit can help alleviate these concerns. The transition of this change will lead to a smooth implementation of the unit and can mean success for investigators and the public. A critical consideration for the implementation of this plan is the length of time needed for the unit to be functional. Change does not occur overnight, and this transition period is no exception. It may be several years before the unit is established and able to impact events or trends described in the three short stories. Also, the occurrence of an event and significant change in a trend can cause the plan to be modified both in brevity of time or prolongation. It is fundamentally important, however, that the plan eventually be implemented.

### Epitaph?

Computers form a common bond with all people, particularly when the vast majority will have access to them. In an interview with Isaac Asimov, he stated that computers will reduce brain numbing work allowing more time for other activities and more toward learning. Interactive devices will emerge to occupy free time. This will enhance the learning atmosphere and people can learn because of the pleasure involved.<sup>27</sup>

This article has shown that computer crime is becoming a serious threat to society . . . more serious than today's occurrences. The trends and events have painted a picture which, if allowed to happen, can lead to tragic consequences. A proactive idea of establishing a joint computer crime team was developed in order to mitigate the undesirable outcome of the trends and events. Lastly, a plan designed to implement the idea was delineated for the purpose of allaying any resistance to change and ensuring a successful transition.

Someone will have to contend with computer wizards who cover their tracks and evade detection. Businesses may become bankrupt because computer pirates are stealing their assets. Will society keep pace with technological change and will governments or politicians allow law enforcement to do so? By the year 2000, law enforcement's Armageddon may very well be the collision of information, computer technology, and the computer criminal. Consider this quote from the book Sneakers, which was also a major motion picture:

The world runs on information--it's the one true international currency.  
This is pure power, the main vein to the universal juice, all of it.

Cosmo moved in close, speaking with great urgency. "The world isn't run by weapons anymore, Marty," he said. "Or oil, or even money. It's run by little ones and zeroes. Little bits of data. It's all just electrons." . . . it's about who controls the information.<sup>28</sup>

## Endnotes

<sup>1</sup> French, Desiree, "Scams Flourish in Electronic Filing System," USA Today (June 15, 1992): 3B.

<sup>2</sup> Associated Press, "Freeway Phone Gets \$1,600 Bill," Fresno Bee, (October 24, 1992): A3.

<sup>3</sup> Media Report, "Phrack Attack," Datamation (December 15, 1990): 29.

<sup>4</sup> Saavedra, Tony, "Firms Hit by Young Hackers Take a Toll on Family Finances," Fresno Bee (February 19, 1993): A3.

<sup>5</sup> Vobejda, Barbara, "Technology Whittles Down Number of Farmers," Fresno Bee (June 14, 1992): E1.

<sup>6</sup> Fall Motoring Special Advertising Section, "Phones, CD's, Luxury Touches Make Cars More Like Home," Fresno Bee (October 17, 1991): 8.

<sup>7</sup> "Gadgets Ahead of Their Time," San Francisco Examiner (Feb. 2, 1992): E-4.

<sup>8</sup> Corcoran, Cate, "Voice Recognition Moving Down To PC's," Infoworld (Nov. 11, 1992): 33.

<sup>9</sup> Vernaci, Richard L., "Phones Getting Smarter," San Francisco Examiner (Dec. 29, 1991): E-12.

<sup>10</sup> Lininger, Skye, "Mobile Office is Reality of '90's," Los Angeles Times (Dec. 7, 1992): C-14.

<sup>11</sup> Cornish, Edward, "Issues of the 90's," 1990 World Future Society (Bethesda, MD: 1990), 10.

<sup>12</sup> Taylor, Charles, Presentation at the Command College Graduation for Class 15 (San Marcos, CA: Jan. 15, 1993).

<sup>13</sup> "Outlook '92 and Beyond: Recent Forecasts from the Futurist Magazine," World Future Society, (1991): 2.

<sup>14</sup> Budwey, James N., "Information Industry in Transition," Internet (February 1992): 2.

<sup>15</sup> Stephens, Gene, "High-Tech Crime Fighting," The Futurist (July-August 1990): 20-25.

- <sup>16</sup> Notes and Handouts, "Criminal Investigation in an Automated Environment," Federal Law Enforcement Training Center (Glynco, VA.: Dec. 3-14, 1990).
- <sup>17</sup> Coutourie, Larry, "The Computer Criminal: An Investigative Assessment," FBI Law Enforcement Bulletin (Sept. 1989):19-22.
- <sup>18</sup> Watson, Neil, "Can Today's Hacker Laws Work?" Communications Week (Sept. 18, 1989): 32.
- <sup>19</sup> Top of the Week, "Phone Fraud: Somebody's Got to Pay," Information Week (May 6, 1991): 12-13.
- <sup>20</sup> Vobejda, Barbara, "How Electronic Gadgetry is Changing Childhood," San Francisco Chronicle (July 30, 1991): D3.
- <sup>21</sup> McEwen, J. Thomas, "Computer Ethics," National Institute of Justice Reports (January-February 1991): 8-11.
- <sup>22</sup> Rayl, A. J. S., "Secrets of the Cyberculture," Omni (Nov. 1992): 59-67.
- <sup>23</sup> Zimmerman, Michael R., "Drug Dealers Find Haven in On-Line Services," PC Week (March 4, 1991): 43.
- <sup>24</sup> NA, Software Industry Bulletin vol. 8 (Nov. 9, 1992): 3.
- <sup>25</sup> Mark Haynes, Interview with author, March 23, 1993.
- <sup>26</sup> Webster, Barbara A. and J. Thomas McEwen, "Assessing Criminal Justice Needs," National Institute of Justice (August 1992): 4-5.
- <sup>27</sup> Coursey, David, "Asimov: Future Computers Will Make Work Fun," MIS Week (Nov. 6, 1989): 44.
- <sup>28</sup> Lasker, Lawrence, and Walter F. Parkes, Sneakers (New York: Signet, 1992), 198.