

POLICE EXECUTIVES MANAGING WITH
COMPUTERS . . . WHERE WILL WE BE IN 1995?

AN INDEPENDENT STUDY PROPOSAL

BY

CAPTAIN LARRY D. HANSEN

LODI POLICE DEPARTMENT

COMMAND COLLEGE CLASS 5

NOVEMBER 1987

Copyright 1988
California Commission on Peace Officer
Standards and Training

TABLE OF CONTENTS

ACKNOWLEDGEMENTS.....	i
EXECUTIVE SUMMARY.....	ii-iii
I. BACKGROUND.....	1-3
II. OBJECTIVE ONE	
Statement.....	4-5
Methods Identification.....	6
Literature Review.....	6-7
Individual Review.....	8
Synopsis of Interviews.....	9-12
Futures Wheel.....	13
Brainstorming Group Sessions-Trends.....	14-30
Events.....	31-37
Cross-Impact Analysis.....	38-47
Scenario Development.....	48
Scenario 1 - Hypothetical (Worst Case).....	49-51
Scenario 2 - Normative (Best Case).....	51-59
Scenario 3 - Exploratory (Most Likely).....	59-65
III. OBJECTIVE TWO	
Statement.....	66
Methods Implementation.....	67-70
Policy Considerations.....	71-72
Stakeholder Identification Analysis.....	72-79
Stakeholder Evolution.....	80
WOTS-Up Analysis.....	81-82
Resource Analysis.....	83
Human Resource.....	84
Mission.....	85
Execution.....	85
Alternative One.....	86-87
Alternative Two.....	87-88
Alternative Three.....	88-89
Recommended Alternative.....	89-90
Administration & Logistics.....	90-91
Funding.....	91-92
Planning System Matrix.....	93-94

IV.	OBJECTIVE THREE	
	Statement.....	95
	Methods Identification.....	95
	Methods Implementation.....	95
	Critical Mass.....	95-100
	Readiness Capability Chart.....	101
	Transition Plan.....	102-104
	Conclusion.....	105-107
	END NOTES.....	108-109
	BIBLIOGRAPHY.....	110-113
	APPENDICES	
	Appendix A Dr. William Tafoya Interview.....	114-118
	Appendix B David J. Roberts Interview.....	119-123
	Appendix C Dr. Ernie Hernandez Interview.....	124-128
	Appendix D Allen L. Pearson Interview.....	129-132
	Appendix E Trends.....	133-136
	Appendix F Trend Screening Form.....	137-142
	Appendix G Trend Evaluation Chart.....	143
	Appendix H Events.....	144-147
	Appendix I Stakeholders.....	148-149

ACKNOWLEDGEMENTS

The feeling of relief at the conclusion of this project is exceeded only by the degree of indebtedness one feels for those who made it possible.

My fellow co-worker, Linda Sunday-Porterfield has been my sounding board, editor, humorist, critic and mentor; without whom I would not have completed this project.

For my Chief, Floyd Williams, who has wondered a thousand times, where's Captain Hansen? My deepest appreciation for your patience and support.

For my academic advisor, Dr. James Hernandez, who was gracious enough to work with a procrastinator and subsequently give so freely of his time and expertise; thank you.

For my secretary, Jacqueline Hodson, who typed and retyped and retyped and retyped; my heartfelt thanks. (The feeling will come back to your fingers Jackie, I promise.)

For Dr. William Tafoya and Doug Dowden who both gave above and beyond any assistance I could have expected from such a degree of expertise, my wonderment and admiration.

For the graphic displays presented in this project I am grateful for the following individuals who came to my rescue; Richard Prima, Mark White, Rick Kiriu, Kay Tamura and Corey Mah.

And last but not least for the guidance, support and encouragement from Doug Thomas, Jan Duke and Everitt Johnson, my appreciation and grateful thanks.

EXECUTIVE SUMMARY

EXECUTIVE SUMMARY

Historically law enforcement has not seen itself as a business, but that is exactly what law enforcement is. We produce a product and supply a service. Our product is a safe community, or if we are faulty in our production, perhaps an unsafe community. Our service is the apprehension of those who threaten another's safety, or who threaten their own. Law enforcement's reluctance to see itself as a business has translated into underuse of technologies which enhance the business process. Law enforcement must embrace these technologies to maximize the effectiveness of its business.

The research for this monograph started with a concept that was refined into the following question: Police Executives Managing With Computers ... Where Will We Be By 1995?

The main focus is to examine the extent to which computer technology can enhance management's capabilities.

The first objective distilled a list of emerging trends and future events into five final considerations; these were considered worthy of future projections. These trends and events are identified as follows:

Trends

1. Computerized law enforcement functions
2. Hardware technology expands through use of portable computer
3. Software technology exponentially advances through artificial intelligence
4. Law enforcement's inundation with information
5. Big brother syndrome - public fear of privacy invasion

Events

1. Public interest group wins civil judgement against law enforcement agency for misuse of automated information
2. Computer hacker arrested for accessing and pirating a police agency's various data base files
3. POST mandates computer training in all California police academies
4. Governor signs legislation which makes funds available for computerization of all California law enforcement agencies
5. Computer vendor perfects voice recognition/activation in portable computers and offers municipal government discount.

These trends and events were then analyzed through various techniques and the extrapolated knowledge was developed and projected into three future scenarios. The second objective of the monograph moves through an analysis process that outlines a basic strategic plan to bridge the gap between the present and the future depicted scenarios. An alternative was identified that provides a guide for law enforcement managers to prepare for the future. And finally, the third objective outlines an implementation plan which is presented to help facilitate the process.

BACKGROUND

PROJECT BACKGROUND

This project is a futures oriented projection of how police executives can manage with computers, with a focus on where we will be by 1995.

The writer's interest in this topic stems from the recent personal experience of automating his police department. Like the majority of police managers today, the writer had absolutely no prior experience with computers. Thus, many trials and tribulations were experienced while fumbling along the path toward automation. Subsequently, the first goal of this research project was to pass along to law enforcement the different perspectives now gained. The second focus was from a realization that police managers are easily deterred from the use of computer technology which has curtailed the progression of computer utilization. Finally, what peaked the writer's interest in this topic, was the interaction with Dr. William Tafoya at the 1987 Law Enforcement Information Symposium in Bethesda, Maryland.

The main focus of this monograph is to examine the extent to which computer technology can be integrated into police management. Although the underpinnings of this study focus on management perspectives, the use of computer technology became naturally intertwined.

Law enforcement's reluctance to view itself as a viable business has meant that certain concepts which enhance business practices have not been embraced by the law enforcement community.

The transformation has been slow but steady, and the writer anticipates a more accelerated acceptance of the business view among law enforcement professionals. College

degrees are now being offered in the management of information. It is the writer's view that an emerging trend among police managers today is a growing recognition of their role as managers of information. Once that premise is widely accepted, the natural evolution will be the use of automation by police managers.

In the business side of law enforcement, management of the workers (police officers) is as paramount as the diverse information to be managed. It is this writer's view that the technology available will lend itself to more effective use of manpower resources in the course of handling the police business.

Because law enforcement managers are becoming increasingly more information-driven, they will more readily accept the tools of automation out of necessity rather than choice.

The premise of this study is that the use and acceptance of computers are accelerating at such a rate that the day will come when managers will not be able to effectively manage without them.

As one recent projection states, by 1990 40-50% of America's work force will be using electronic terminals daily.

Police "professionalism" primarily stresses efficiency and technical competence in crime control as one of its major tenets. Implicitly, this dimension of reform requires a centralized, systematic information gathering process.(1)

Although we are well into the computer revolution, we in law enforcement haven't begun to discuss how to manage computer operations. In fact, most of us are still trying to figure out what a computer is.(2)

Automation provides a kind of catalyst for reform where the system itself demands or requires change in management and various organizational roles, or distributes power through subtle changes in information flow.(3)

Today we assume that everyone we deal with has a telephone; soon we may be able to assume that everyone we deal with has a computer.

This monograph utilizes a variety of projection techniques which massaged and refined the main issue.

This process created a vision of where we've been, where we are and where we're going. Looking over this panorama provides a perspective that takes one from where we were (when the telephone was high technology and the calculator was expensive and sought after). This naturally progresses to where we are; computers are no longer unique, but their usefulness is still being explored as we seek applications to convert to automation. Managers are charged with the responsibility of insuring that managerial enhancements are commensurate with the technological advancements. This monograph, then helps to guide us through where we are going, and one path for how we may get there.

This writer now intends to illuminate for the reader a series of possibilities facing police managers as they approach 1995. An overview of issues shaping these paths is addressed as part of the journey police managers embark on when considering the automation of information.

OBJECTIVE ONE

OBJECTIVE ONE

Statement

The first objective is to factor and study the general issue utilizing futures research methodologies. The outcome of the study will be three future scenarios. The general issue is: "Police Executives Managing With Computers . . . Where Will We Be by 1995?"

Through the process of brainstorming exercises, involving other Command College students and my NGT group, numerous related issues were discussed. By the process of consensus three past related issues have been identified as significant and worthy of reflection. They are as follows:

1. What really influenced the computer movement in the police arena?
2. What financial impact did computerization have on police organizations?
3. In the beginning, what limitations has law enforcement had on computer technology?

The technology issue is still viable today because of the volumes of information that law enforcement needs to collect, process, store, analyze and retrieve.

Related issues emerging in the present were identified through the same brainstorming technique. They are as follows:

1. How can police organizations finance computer technology?

2. How can law enforcement executives use computer technology to manage human and financial resources?
3. How can law enforcement executives identify hardware and software that will best meet their individual needs?
4. How can law enforcement avoid and/or counter the general public's concern about the "Big Brother Syndrome"?
5. How can law enforcement managers impact the competency level and subsequent acceptance of computers with new recruits?

The issues were then subjected to a preliminary screening, as an approach to structuring the general issue for research. The criterion was a judgement concerning degree of relatedness. The result was a list of three issues that, when considered together, essentially define the parameters of the general issue being studied:

1. How will law enforcement managers be able to use computer technology to enhance their own level of knowledge and expertise?
2. How will computer technology assist law enforcement managers in matching personnel to specific jobs (assignments) and the training of personnel for those jobs?
3. How can computer technology assist managers to identify community concerns that may require proactive responses?

Consideration was given to a related issue that might emerge by the year 1995. This issue was judged to be

relevant on the basis of potential impact upon possible future scenarios. The issue was identified as: Will the advent of artificial intelligence impact police management as we know it today?

Methods: Identification

The formation and design of this monograph is based upon a multifaceted course of study that was presented through Command College, an executive development program sponsored by Peace Officer Standards and Training (POST).

To improve the probability of the future scenarios and subsequent strategic planning and implementation plan, relevant data was analyzed through the following seven processes:

1. Literature review
2. Individual interviews
3. Futures wheel exercise
4. Brainstorming group sessions
5. Forecasting trends and events
6. Cross-impact analysis
7. Scenario development

Literature Review

The first goal of the process was the development of a comprehensive list of all relevant materials on the subject. However, in the preliminary stages, the amount of material indicated that an all inclusive reference list was impossible to complete within the specified time frame. The

bibliography provided in this monograph is by no means exhaustive but it does provide a sense of the complexity of the issue under study, along with various considerations that might lead to further research. The review of the literature consisted of four primary sources:

1. The Peace Officer Standards & Training (POST) Library in Sacramento, California
2. The Federal Bureau of Investigation (FBI) Library in Quantico, Virginia
3. Computer search by topic heading and various subheadings (electronic database search)
4. Law enforcement information symposium (August 1987, Washington D.C.)

The review of the literature revealed some insights reflective of this issue:

1. The current state of computer technology is in a constant state of flux - new possibilities and capabilities are continually emerging.
2. Many social problems and moral dilemmas will surface through the advancement of this new computer technology.
3. The demand for management competency in systems approach, implementation and computer literacy will continue to increase inevitably because managers will not be able to effectively manage without this level of knowledge.

4. Computer technology represents an opportunity par excellence of police management impacting the efficiency of their organization in maximizing the use of information and various controls on productivity.
5. The need of law enforcement to process more and more information necessitates the acquisition of computer technology.
6. Law enforcement leaders who intend not to let the future pass them by, must embrace this technology called computers.
7. Law enforcement managers must learn how to deal with the use and abuse of expanded information accessible by computers.
8. The recently perceived goal of a paperless society and subsequent police department is probably not attainable in the near future (7-10 years).
9. When dealing with computer technology, law enforcement managers should strive to insure that short term decisions are consistent with long term goals.
10. The possibilities and impacts of computer technology on law enforcement are limitless partly because we can not easily predict technology that does not yet exist.

Individual Interviews

Personal interviews were conducted with four authorities in the field of computer technology as it applies to law enforcement. The interview process allowed the continual

refinement of the issues of this study, and allowed the redefinition of both the structure and the research. The outline of the interviews are in Appendix A-D. The experts interviewed are listed in order of initial contact:

1. William L. Tafoya, Ph.D - A supervisory FBI Agent assigned to the Artificial Intelligence Research Project of the National Center for the Analysis of Violent Crime at the FBI Academy in Quantico, Virginia
(703) 640-6131 ext. 1226
2. Dave Roberts - Deputy Director with Search Group, Inc. He is presently working in the Research and Statistics Program (916) 392-2550
3. Ernie Hernandez, Jr., Ph.D. - Author of "The Systems Approach and Computer Technology", and numerous publications in this field. (714) 837-6258
5. Al Pearson - Senior Staff Analyst with IACP, Masters in Urban Studies, 5 years experience at the Institute of Police Technology and Management as a Micro Computer Section Coordinator. (904) 646-2722

Synopsis of Interviews

Given the opportunity to interview experts in the field of computer technology provided valuable insight to the main issue of this monograph. The interviews were by no means a scientific analysis of data, but they did provide some meaningful insight. The entire interview content is included

in Appendix A-D. The questions asked of all four participants were as follows:

- 1) What percent of law enforcement agencies in California have some form of automated crime information system?
- 2) Do you view a paperless society and/or a paperless policy department as a viable possibility within the next seven years?
- 3) Do you feel law enforcement can effectively deal with computer crime both today and in the future?
- 4) Do you foresee a "big brother" issue surfacing to the point that law enforcement use of computers will be curtailed?
- 5) Do you think the State of California, through legislation, will provide funding or incentives to assist law enforcement agencies who want to automate?
- 6) Are you aware of any agency that can assist a law enforcement agency who is considering automation?
- 7) Do you foresee a governing body legislating law enforcement's use of computers?
- 8) Do you foresee police agencies interfacing (exchanging crime analysis type of information) in a statewide network?
- 9) Do you think law enforcement agencies are being monitored by computer hackers?

10) In what ways do you foresee law enforcement executives using computers to manage, a scenario if you will?

As a result of the interviews the writer learned that no one really knows how many agencies in California are automated. The best guess is that approximately 1/3 have some form of automation. It should be noted however, that 81% of California's police agencies serving a population of 100,000 or more have some form of automation.

It does not appear that a paperless police department is a viable possibility in the near future.

There was an overall consensus that law enforcement agencies today are not equipped or trained to effectively deal with computer crime. Three of the experts saw the potential of a big brother issue surfacing and the fourth, Dr. Tafoya, saw a definite likelihood of this event occurring. He cited some current activities that have recently developed in Washington, D.C.

There was not much of a possibility seen for a state government agency providing funds to local agencies to automate.

There are several agencies on the state and national level that can assist law enforcement agencies who are considering automation;

- 1) Search Group, Inc.
- 2) IACP

- 3) National Criminal Justice Reference Center
- 4) Institute of Police Technology and Management

There was not an immediate concern about a governing body legislating law enforcement's use of computers, but it was seen as a possibility.

There was a mixed response on the possibility of a state wide computer network. There was a consensus that it would be a difficult process.

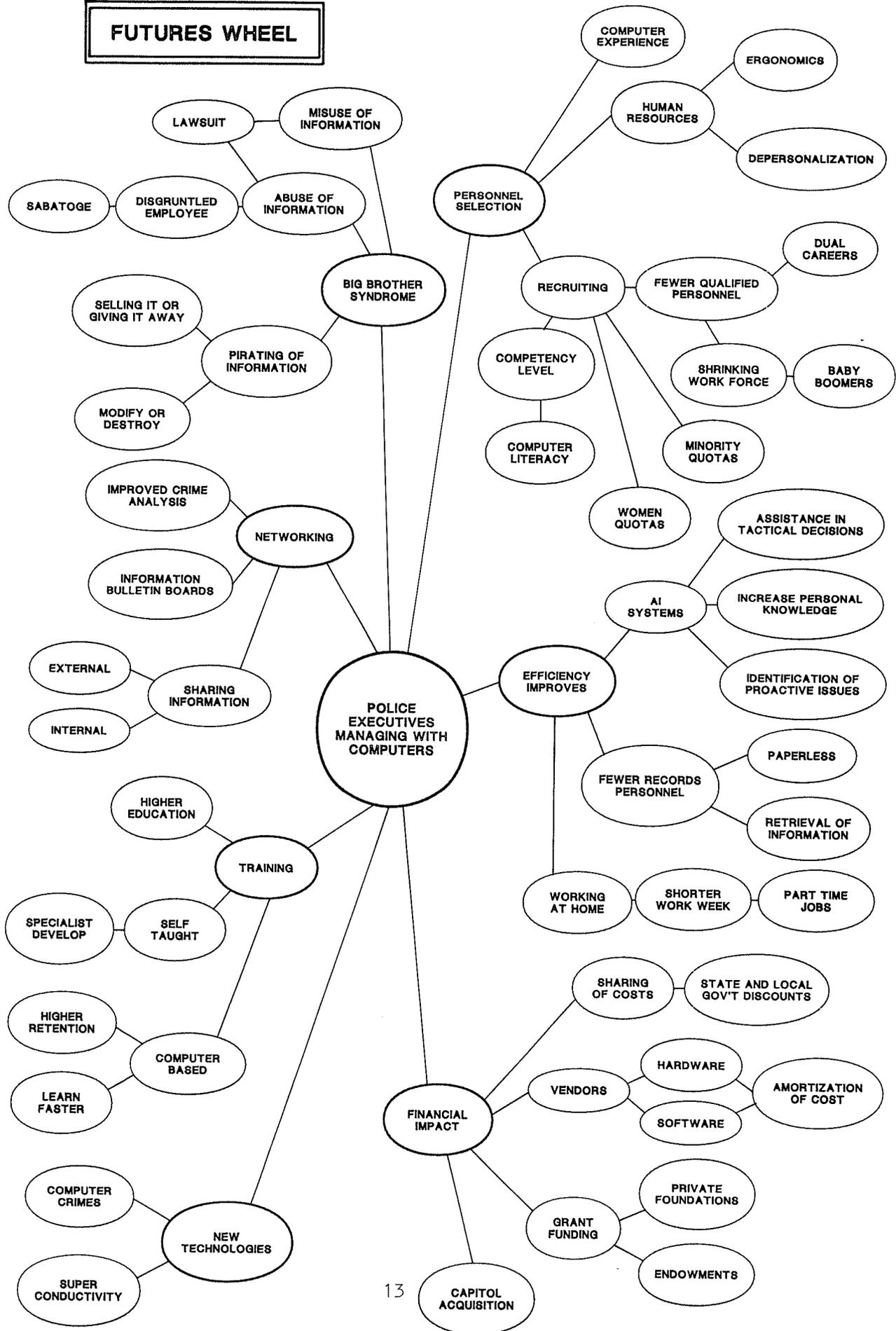
There was a consensus that the possibility of a computer hacker infiltrating a law enforcement computer system, but not to any great extent.

There was a variety of responses on how the future use of computers to assist managers in their daily operations. A general consensus prevailed that law enforcement managers must be prepared for the new capabilities as they emerge.

Futures Wheel

The futures wheel exercise is a tool used to explore relevance of an issue, and focus on related trends. This exercise enables participants to brainstorm the main issue and expand it in any given direction perceived relevant.

FUTURES WHEEL



Brainstorming - Group Sessions

This simple but effective analytical process enabled me to focus on past and present developments, previously mentioned and on emerging trends and events. On the first occasion I met with some of my fellow Command College students and initiated the process. I used this group primarily for their law enforcement experience. Building on their education and experience provided a foundation on which to prepare for the session with my NGT group.

The individuals that participated in the NGT group had extensive backgrounds. This group had a combined total of 65 years of experience in a broad range of computer-related occupations. The participants in this group are identified as follows:

Lynndee Riley-Black - Systems Engineer with IBM

Martin Jones - Programming Supervisor, City of Stockton

Roy Todd - Data Processing Supervisor, City of Lodi

Linda Porterfield - Planning and Research Coordinator,
City of Lodi

Doug Dowden - Chief Executive Officer of DLH-INE, Inc.
(computer software company currently used by Lodi Police
Department and 24 other law enforcement agencies)

Facilitation of the brainstorming process led to an extensive list of "potential" trends that are relevant to the main issue of this monograph. The group was given the following basic guides for consideration when discussing

potential trends and events: events are discrete occurrences - they are things that either happen or do not happen - while trends are the patterns of happenings over time. Events should be stated so that a future historian, looking back over time, could clearly tell whether or not they had, in fact, happened. Conceptually, trends are the fundamental descriptors of any future, and hence they must be defined carefully. Through the brainstorming technique a list of 69 trends was developed (refer to Appendix E).

After the 69 trends were listed in the brainstorming session each NGT member rated these trends using a trend screening form (Appendix F). They were asked to estimate the value of each trends importance in terms of police executives managing with computers. Each member was then asked to individually pick five trends from either the "helpful" or "very helpful" column. Through an informal voting process the group reached a consensus on five trends collectively viewed as most worthy of futures forecasting. These trends were identified as follows:

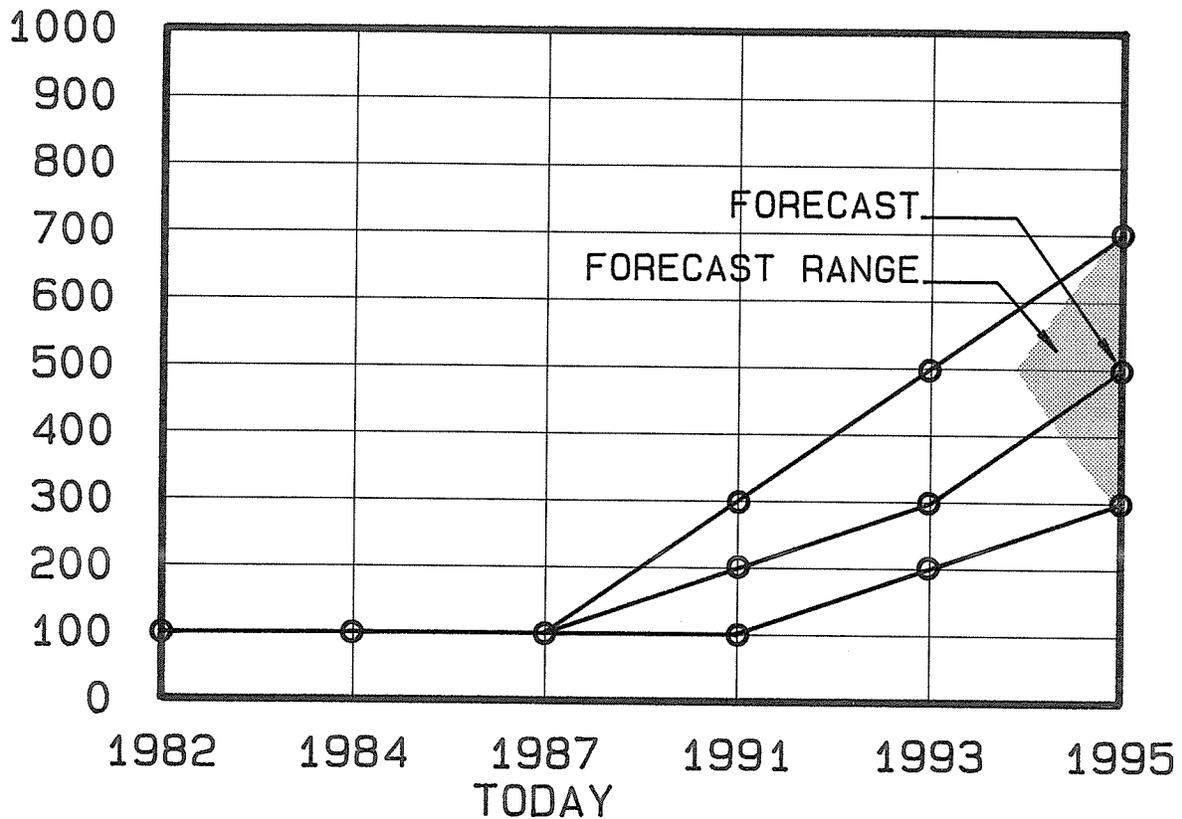
- 1) Computerized law enforcement functions
- 2) Hardware technology expands through the use of portable dumb terminals
- 3) Software technology exponentially advances through artificial intelligence
- 4) Law enforcement's inundation with information
- 5) Big brother syndrome - public fear of privacy invasion

Through the use of a trend evaluation form (Appendix G) and using the numerical rating of 100 as today's level, each member projected backwards for five years and then forward for seven years. The seven year standard was divided into a projection of where we "will be" and then where we "should be". Because the advent of computer technology is rapidly changing, almost on a daily basis, the group felt that no more than a seven year projection was reasonable. The following charts represent a consensus of the group's high, low and average ratings for each of the five selected trends.

TREND EVALUATION CHART

TREND STATEMENT	LEVEL OF THE TREND (RATIO: TODAY=100)			
	5 YEARS AGO	TODAY	"WILL BE" IN 7 YEARS	"SHOULD BE" IN 7 YEARS
1. COMPUTERIZED LAW ENFORCEMENT FUNCTIONS	50	100	500	700
2. HARDWARE TECHNOLOGY ADVANCEMENT - BRICK "DUMB" TERMINALS	0	100	600	700
3. SOFTWARE TECHNOLOGY- EXPONENTIAL ADVANCEMENTS THROUGH ARTIFICIAL INTELLIGENCE	20	100	800	1,000
4. INFORMATION INUNDATION IN LAW ENFORCEMENT	40	100	500	700
5. BIG BROTHER SYNDROME (PRIVACY INVASION)	30	100	200	100

TREND: COMPUTERIZED LAW ENFORCEMENT FUNCTIONS



ESTIMATED TREND VALUE FOR TODAY -100%

In an era of increased demands for efficiency, law enforcement has turned to automation because of the volumes of information that must be stored, processed and retrieved. Public demand for hardware and software has resulted in decreasing costs which makes computers affordable for even the smaller agencies.

The group was informed that today, approximately 1/3 of California's law enforcement agencies are fully automated.

The current capabilities of most computerized law enforcement systems may include any of the following functions:

CAD - Computer Aided Dispatch (police and fire)

Records Management Information System

Crime Analysis Information System

Criminal Investigations System

Jail/Booking/Court System

1987 - 1991

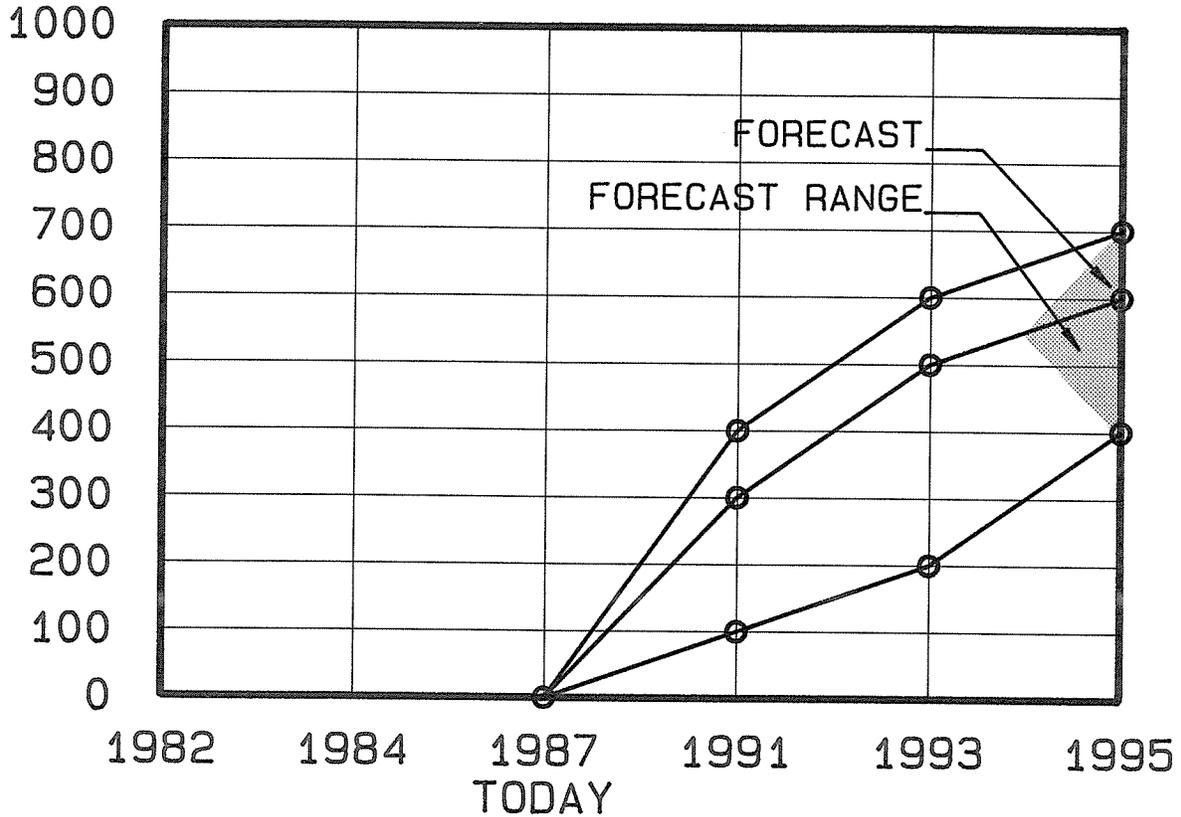
The group consensus was that computer technology provides the means for greater efficiency, but more importantly, greater effectiveness for organizations that must process large quantities of information. It was felt that the expansion of computer technology would continue to increase and the group forecasted the trend would move to two hundred percent (200%) by 1991.

1991 - 1995

The computer is becoming a major factor and as it continues to be refined and upgraded, it may become the most dominant factor in policing since the patrol car.(4) Policing will change, of course, but in many ways it will remain the same. Police will have considerable help from the computer and other advanced technologies.(5)

There was a group consensus that in this 4 year time span a majority of police agencies will recognize that automation is a necessity and will embrace the variety of technological advancements. The group supported the premise that use and acceptance of computers are accelerating at such a rate that police managers will not be able to effectively manage without them. The group consensus was that the trend of computerized law enforcement functions would escalate to five hundred percent (500%) by 1995. The group assigned a high estimated trend value to this issue for today at one hundred percent (100%).

**TREND: HARDWARE TECHNOLOGY ADVANCEMENT
-BRICK "DUMB" TERMINALS**



ESTIMATED TREND VALUE FOR TODAY-70%

Technology has been developed and currently "dumb" terminals are utilized on a limited basis. The terminals are linked via radio waves to mainframe units. These terminals currently operate on cellular networks (the same system cellular phones use). They also have the capability of networking through satellites, and/or fiber optics. These terminals, currently being used by IBM and Motorola, are

basically a little box about the size of a brick. It is a fully self-contained terminal with a radio transmitter and receiver. The terminal has a keyboard and display screen, but networks with a main computer replete with all the capabilities of the CPU. The current rage today is micro computers, but these pale in comparison with the technological capabilities of the brick terminals. The only limitation of the brick terminal will be the limits of the computer it is networking with.

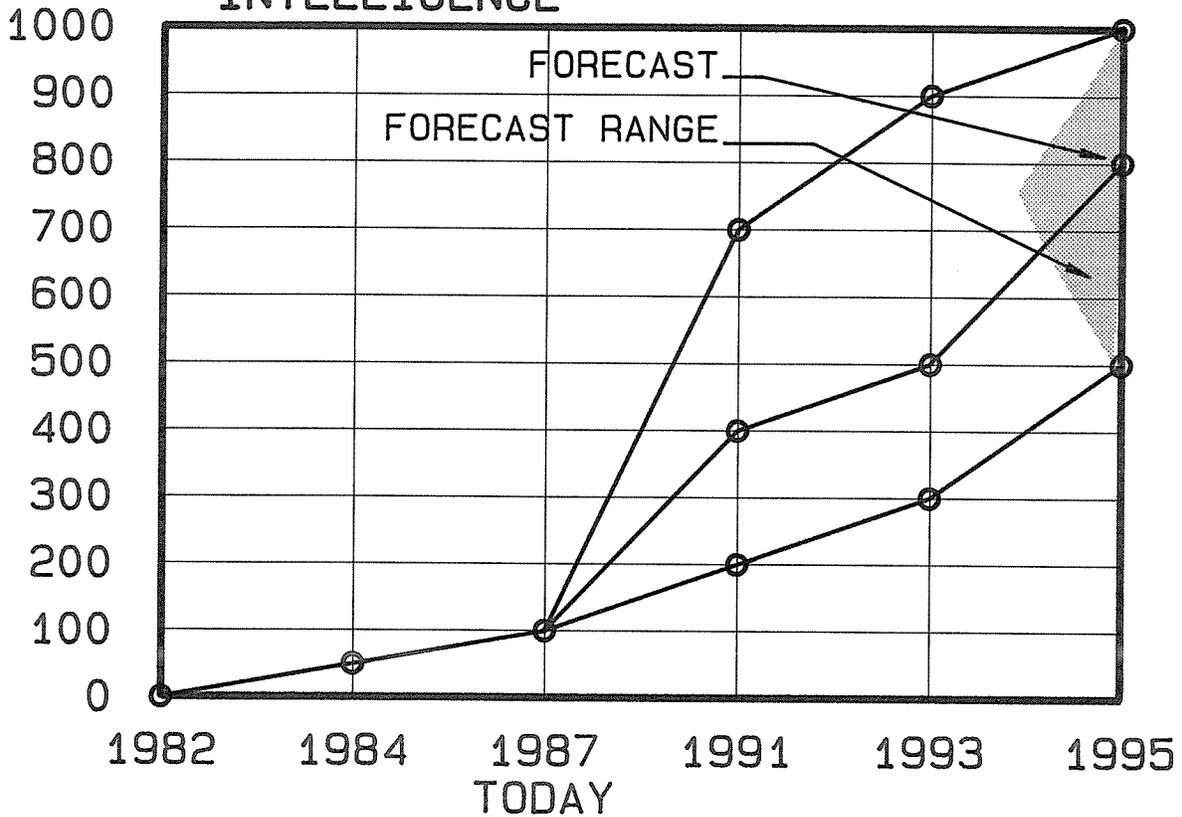
1987 - 1991

The capabilities this technology offers law enforcement are exciting. It will afford officers the ability to immediately access information in the mainframe and/or add and update information again through direct access. The group forecasted an increase in the movement of this trend to three hundred percent (300%) by 1991.

1991 - 1995

The group collectively agreed that a combination of this hardware technology with the software technology of artificial intelligence (which might be enhanced with a natural language identification/generation feature) moved this trend to six hundred percent (600%) by 1995. The group assigned a high estimated trend value of importance to this issue for today at one hundred percent (100%).

**TREND: SOFTWARE TECHNOLOGY-EXPONENTIAL
ADVANCEMENT THROUGH ARTIFICIAL
INTELLIGENCE**



ESTIMATED TREND VALUE FOR TODAY-100%

Although still in its infancy, artificial intelligence (AI) promises to be one of the most exciting scientific disciplines.(6) An explosion appears certain within the next five to ten years.(7) Basically, artificial intelligence is concerned with developing computer systems that generate the types of results normally associated with human intelligence,(8) (specifically emulating the behavior of

human experts). The goal - often referred to as the "fifth generation" computer - is a system that operates at extremely high speeds, does not require users to remember complex codes and commands, communicates in natural or "human" language and most importantly, learns from its own experience.(9)

Artificial intelligence holds the promise of a number of quite different and specialized technologies:(10)

1. Robotics - machines with sensory capabilities that can detect and recognize sounds, pictures, textures, heat, cold, etc.
2. Knowledge-based systems - computer systems which contain a large quantity of information on a subject and that can be queried to solve problems.
3. Expert systems - computer systems designed to replicate the problem-solving skills of expert practitioners in a specific field.
4. Natural language identification/generation systems - programming and hardware that can understand human language and respond to inquiries in human language.
5. Computer-aided instruction - when boosted by artificial intelligence, CAI can resemble a socratic dialogue between teacher and pupil.

1987 - 1991

Drawing on this introduction to artificial intelligence the group saw tremendous potential to impact the main issue of this monograph - managing with computers, the group

estimated a movement, in this time span, from one hundred percent (100%) to four hundred percent (400%).

1991 - 1995

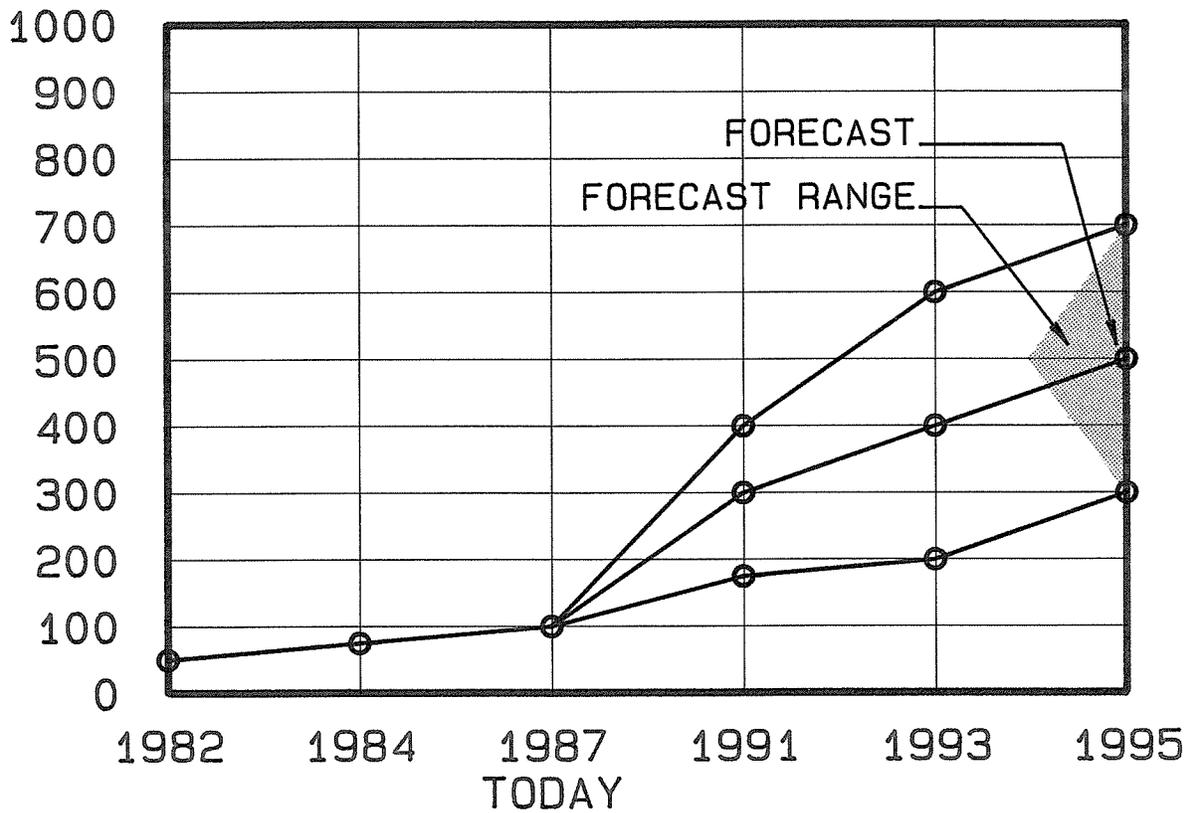
At the 1987 Law Enforcement Information Symposium in Bethesda, Maryland, Dr. William Tafoya, an FBI Academy Instructor, outlined potential criminal justice applications of artificial intelligence. Dr. Tafoya related two specific applications the FBI is currently working on. The first is an expert system to be used in white collar crime investigations and the second a serial murder expert system. The FBI will soon start development on profiling other violent crimes such as rape and child molestation.(11) Dr. Tafoya felt that artificial intelligence would seem to lend itself well to the following law enforcement applications: telecommunications, administration, training, personnel matters, performance appraisal, equipment and evidence inventory, preventive maintenance, legal issue analysis and tracking of training courses. Artificial intelligence may offer the greatest potential to law enforcement in the area of training. With standardized computer based instruction (CBI), it will be possible to testify that this officer received this precise training at a stated level of competence.(12)

The consensus of the group was that with artificial intelligence systems developed during this four year time span the possibilities for applications in law enforcement

were limited only by one's imagination. The group saw an exciting escalation of this trend from five hundred percent (500%) in 1993 to eight hundred percent (800%) by 1995.

The group assigned the maximum of one hundred percent (100%) for today's estimated trend impact value on the issue.

TREND: INFORMATION INUNDATION IN LAW ENFORCEMENT



ESTIMATED TREND VALUE FOR TODAY - 90%

Today, 60% of the American labor force have jobs creating, processing or distributing information(10?). While the shift from an agricultural to an industrial society took 100 years, the present restructuring from an industrial to an information society has taken only two decades.(13) In the information society, we have systematized the production of knowledge and amplified our brain power. To use an industrial metaphor, we now mass produce knowledge and the knowledge is the driving force of our economy.(14)

The combined technologies of the telephone, computer and television have merged into an integrated information and communications system that transmits data and permits instantaneous interactions between persons and computers.(15)

A personal example of the growth of information was given to the group. In 1985 the Lodi Police Department (considered a medium size department with a compliment of 91 employees serving a population of 48,000) went on line with a new computer system. The system had 716k of internal memory and 400mb of hard disk storage. It was estimated the system would handle the information processing of this agency for approximately 3-4 years. In reality the agency outgrew the system in 15 months which necessitated expanding to a faster, larger system.

1987 - 1991

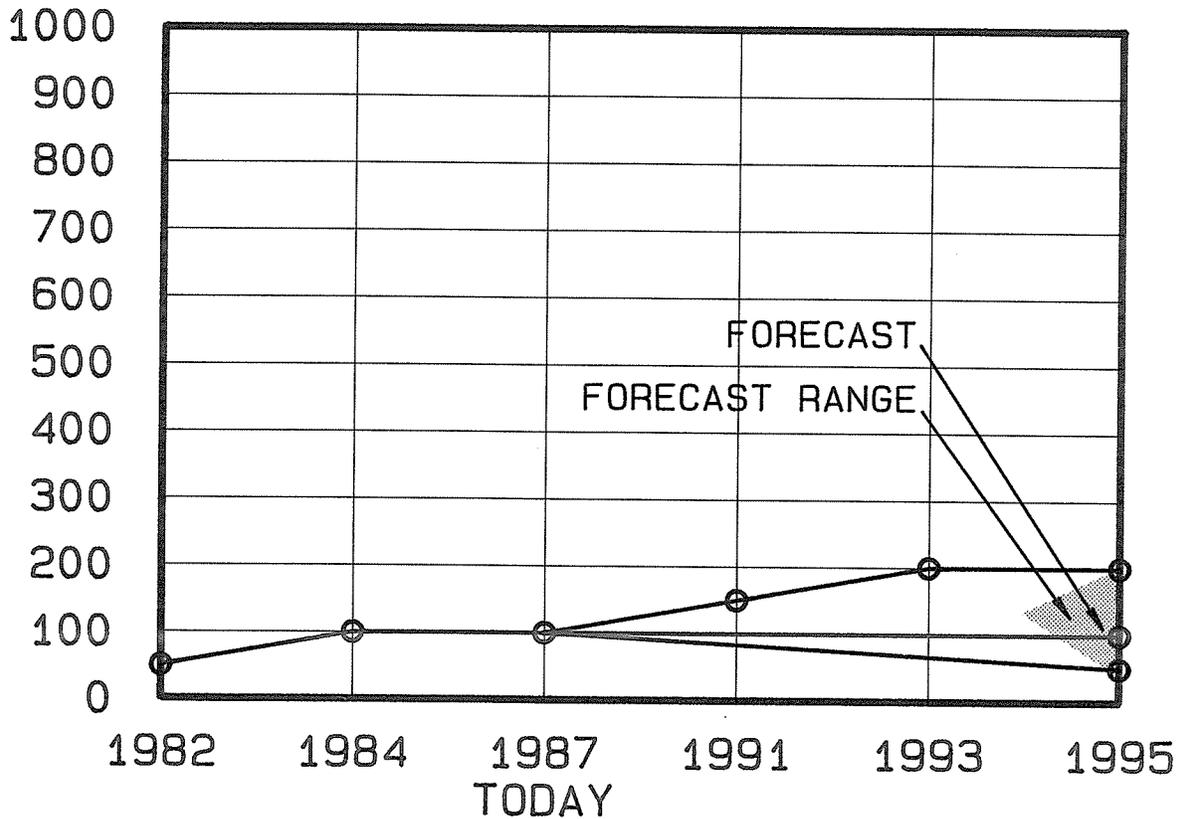
Law enforcement is in the business of processing information. The group consensus is that the volumes of

information that will need to be processed, stored and retrieved will continue to expand. The group forecast a movement in this trend from one hundred percent (100%) to three hundred percent (300%) by 1991.

1991 - 1995

With the technologies available by 1991, the processing of information will escalate at a rapid rate. The forecast of this trend moves significantly to five hundred percent (500%) by 1995. The group assigned a high estimated trend value to the issue for today of ninety percent (90%).

TREND: BIG BROTHER SYNDROME- (PRIVACY INVASION)



ESTIMATED TREND VALUE FOR TODAY-60%

Many times each day the following scenario occurs: an officer questioning a crime victim asks: "Name, please?"
Victim: "John Jones." Officer: "Age and date of birth?"
Victim: "Why do you need to know that?" Officer: "It's for the crime report."
Victim: "I don't see why that's relevant."

Two areas of concern emerge when examining the "Big Brother Syndrome"; 1) invasion of privacy, and 2) misuse of acquired information.

The example of unlisted phone numbers is indicative of many who choose not to share personal data in a public forum. The reluctance of some to obtain credit cards may be to avoid being placed in a massive data network.

Some individuals who have been victimized are reluctant to report the crime to the police and subject themselves to what they see as further victimization.

Posse Comitatus and similar groups are often challenging law enforcement's right to information citing past misuse, and basing their claims on constitutional issues.

1987 - 1995

Given the criteria of 100 as today's value, the group foresees this trend remaining at 100 through the next seven years. If this trend rises, the group foresees that as a negative reflection on law enforcement's use of information. If this trend declines, it will be indicative of a positive reflection on law enforcement's use of information. The gauge for measurement of this trend lies in whether or not restrictions are imposed on law enforcement's access to information. If legislation or a court ruling were to narrow law enforcement's right to information, it may well be due to failing to protect our public's privacy. The group feels a

trend value of 100 in 1995 will demonstrate that the level of confidence we enjoy today has been maintained.

In another effort at brainstorming the group generated a list of critical events that could have an impact on the issue by either accelerating it or diffusing it to a significant degree (refer to Appendix H).

After the NGT group generated the list of 31 events, a lengthy discussion distilled the list to a final set of five. It was agreed that if these events were to occur they would significantly impact the main issue of police executives managing with computers. And, if that premise is sound, then these five events are worthy of forecasting for some insight into the future. The five events are listed as follows:

- Event 1 - Public interest group wins civil judgement against law enforcement agency for misuse of automated information.
- Event 2 - Computer hacker arrested for accessing and pirating a police agency's various data base files.
- Event 3 - POST mandates computer training in all California police academies.
- Event 4 - Governor signs legislation which makes funds available for computerization of all California law enforcement agencies.
- Event 5 - Computer vendor perfects voice recognition/

activation in portable computers and offers municipal government discounts.

The group was next asked to decide the year that the probability for each event first exceeds zero. Each group member then assigned a numerical percentage to each event indicating the probability of that event occurring by 1991 and 1995. The group member then assigned a numerical rating, on a scale of -10 thru +10, that each event would have on the issue area and the net impact on law enforcement. The following event evaluation chart displays the median probability of each event in the listed categories.

EVENT EVALUATION CHART

EVENT STATEMENT	PROBABILITY			NET IMPACT ON THE ISSUE AREA (-10 TO +10)	NET IMPACT ON LAW ENFORCEMENT (-10 TO +10)
	YEAR THAT PROBABILITY FIRST EXCEEDS ZERO	BY 1991 (0-100)	BY 1995 (0-100)		
EVENT 1. CIVIL SUIT JUDGEMENT AGAINST LAW ENFORCEMENT	1989	20%	50%	-4	-5
EVENT 2. COMPUTER HACKER PIRATES POLICE DATA	1988	30%	50%	-5	-6
EVENT 3. P.O.S.T. MANDATES COMPUTER TRAINING	1990	50%	60%	+9	+10
EVENT 4. LEGISLATION FUNDING COMP. SIG. BY GOV.	1991	20%	40%	+10	+10
EVENT 5. GOV. DISC. ON LANGUAGE GENERATION SYSTEM	1990	40%	60%	+7	+10

Through the exercise of assessing these key trends, the following clarifications were made about each event.

Event 1 - Civil Court Decision

Based on the group's years of experience in law enforcement, it appears that there is a better than even chance that a court will be asked to make a judgment on an agency's misuse of information. To clarify misuse it could

be something as simple as running a registration solely for the purpose of finding the address of a good looking driver, to something as complex as using a vacation check list to enhance the success of a police officer burglary ring.

A recent article in U.S. News and World Report highlighted concerns about the FBI Computer System referred to as "Big Floyd". The chief concern is that "the FBI will tie its computers into the files of other agencies, exponentially increasing the bureau's ability to keep track not only of law breakers but potentially average citizens. In short they ask whether Big Floyd could become Big Brother." Reasonable men will differ on where to draw the line between use and abuse of information. Law enforcement needs to be intuned to this issue before the courts draw the line as they have in other similar issues.

Event 2 - Computer Hacker Pirates Police Data

The odds are in favor of someone, somewhere, capturing information from a policy agency's computer files. On October 31, 1987 there was an article in the New York Daily News (page 9) about how members of the Hells Angels tried to break into the FBI's National Crime Data Bank. An informant testified that their intent was to either delete, add or even sell information in the NCIC Computer. The members were going to use a computer expert to get into the system. Any computer system that transmits information via telephone lines is particularly accessible and subject to being altered

or captured. Any computer transmits electro magnetic radiation and these electronic impulses can be captured and deciphered into an intelligent format given the right piece of equipment. As law enforcement becomes more attuned to computer technology and the various crimes perpetrated by computer hackers, there is a fifty-fifty chance an individual will be arrested for pirating police data.

Event 3 - POST-Mandated Computer Training in Police

Academies

It seems almost inconceivable that there is currently no computer training offered specifically as a performance objective to new recruits in POST-approved police academies. At the time of this writing, POST offers four different certified courses for a combined total of approximately 100 hours of training. These include introduction to computers (24 hours), hands-on training with computers (24 hours), emergency management with computers (18 hours) and computer crime (36 hours). It should also be noted that there are a variety of other POST sponsored courses that focus on a particular aspect of computer technology as part of the course content (i.e. Introduction to Crime Analysis). The group foresees a better than even chance that POST will mandate a minimum number of hours of training in the various aspects of computer technology as a condition of completion of the basic academy course. While interviewing Dr. Hernandez, the writer learned that the Los Angeles Sheriff's

Department will soon include 100 hours of computer training for new recruits as part of the academy program. This program is expected to start in 1988.

Event 4 - Computer Funding Legislation

The best estimate found today is that approximately a third of California's law enforcement agencies have some form of automation. The catalyst for government assistance in funding new agencies will probably be the BCS reporting requirement or a similar function. With the cost of computer equipment decreasing and the advantages of the technology increasing, it seems feasible that the state will provide funding assistance to the smaller agencies who have yet to automate.

Event 5 - Government Discount on Language Generation Systems

The technology of voice activation/recognition computers exists today, but full development is probably a couple of years away. The recognition of various speech patterns is still a major problem as is context interpretation. (i.e. I'm going to the store - to, too, or two.)

However, once this technology is fully developed the impact on law enforcement could be tremendous. Imagine if you will, officers in the field receiving a message from their MDTs in both verbal and printed format.

Cross Impact Analysis

With trend development and critical event probability established a cross impact analysis was initiated. Most

practitioners in futures research now recognize that events should be considered in the context of trends. The result of this analysis will be the identification of potential policy action targets. If a particular event always moves the other events and trends in desirable (or undesirable) direction, then it is clearly a target for policy. If, as is more common, a particular event has mixed effects, both good and bad, then it too may be a policy target. However, the costs and benefits of intervening should be understood before initiating policy changes.

Through this process the following two questions were asked over and over again. 1) If this event (i.e. Event 1) actually occurred, what would the new probability of another event (i.e. Event 2) be at the moment of greatest impact? 2) If this event (Event 1) actually occurred, how great a change, if any, would it have on the projection of this trend (Trend 1) at the point of greatest impact? These influences are called "cross impact". As a result of this analysis the following observations can be made.

CROSS-IMPACT EVALUATION CHART

E V E N T S	NOMINAL PROBABILITY--1995	EVENTS					TRENDS				
		EVENT-1-CIVIL SUIT -JUDGEMENT AGAINST LAW ENFORCEMENT	EVENT-2-COMPUTER HACKER PIRATES POLICE DATA	EVENT-3-P.O.S.T. MANDATES COMPUTER TRAINING	EVENT-4-COMPUTER FUNDING LEGIS SIGNED BY GOVERNOR	EVENT-5-GOVT. DISCOUNT ON LANGUAGE GENERATION SYSTEM	TREND-1-COMPUTERIZED LAW ENFORCEMENT FUNCTIONS	TREND-2-HARDWARE TECH. ADVMT. -BRICK "DUMB" TERMINALS	TREND-3-SOFTWARE TECHNOLOGY-- EXPONENTIAL ADVMT. THRU AI	TREND-4- INFORMATION INUNDATION IN LAW ENFORCEMENT	TREND-5-BIG BROTHER SYNDROME (PRIVACY INVASION)
EVENT 1-CIVIL SUIT- JUDGEMENT AGAINST LAW ENFORCEMENT	50%	X	+40%	+40%	-30%	--	-200%	--	--	-200%	+300%
EVENT 2-COMPUTER HACKER PIRATES POLICE DATA	50%	+30%	X	+20%	-10%	--	-200%	--	--	-200%	+100%
EVENT 3-P.O.S.T. MANDATES COMPUTER TRAINING	60%	-10%	+10%	X	+10%	--	+200%	+200%	+200%	+200%	--
EVENT 4-COMPUTER FUNDING LEGISLATION SIGNED BY GOVERNOR	40%	+20%	+10%	+60%	X	+20%	+300%	+300%	+300%	+500%	--
EVENT 5-GOVERNMENT DISCOUNT ON LANGUAGE GENERATION SYSTEM	60%	+10%	--	+40%	+20%	X	+300%	+300%	+300%	+500%	--

Event 1 - Civil Court Case: Specifically a judge awarding civil damages to a special interest group or individual and

against a law enforcement agency for misuse of automated information.

If this event actually occurred, then Event 2 (computer hacker arrested for piracy) will increase in probability from a fifty percent (50%) chance of occurring to a ninety percent (90%) chance of occurring, in that law enforcement agencies will be more security oriented and will vigorously search for intruders before computer crimes surface through other means.

Event 3 (POST-mandated training) will substantially increase in probability from a sixty percent (60%) chance of occurring to a one hundred percent (100%) chance of occurring in that the need for extensive training will become evident. Event 4 (legislation of funds for automation) will experience a substantial reduction from a forty percent (40%) chance of occurring to a ten percent (10%) chance of occurring because of the political ramifications to funding agencies who may be considering automating in the shadow of a civil case that generates a lot of negative publicity.

This event will have a moderate impact on Trend 1 (computerized law enforcement functions) advancing the impact by two hundred percent (200%) to an overall seven hundred percent (700%) in that the individual law enforcement agencies that are automated may stagnate or if they do continue to expand it will be at a slower pace and those law enforcement agencies that are considering automation may choose to automate fewer functions (choosing only programs

considered an absolute necessity). Event 1 will also have a moderate impact on trend 4 (information inundation) advancing the impact by two hundred percent (200%) to an overall seven hundred percent (700%), in that law enforcement agencies who are inundated will continue to be inundated without automation and law enforcement agencies that are automated may incur additional expense to improve security and train personnel.

Event 1 will have a substantial impact on Trend 5 (Big Brother) advancing the impact by three hundred percent (300%) to an overall five hundred percent (500%). When evaluating the impact of this trend the reader must understand that an increase is seen as a negative reflection on law enforcement.

Event 2 - Computer Hacker Arrested for Piracy:
Specifically a computer hacker is arrested for accessing a policy agency's data base and then selling that information to an unauthorized source (i.e. narcotics dealer).

If this event actually occurred, then Event 1 (civil court case) would be impacted by increasing the probability from a fifty percent (50%) chance of occurring to an eighty percent (80%) chance of occurring in that publicity and subsequent public sentiment will be negative toward law enforcement as a result of this event.

Event 2 would also impact Event 3 (POST-mandated training) by increasing the probability from a sixty percent (60%) chance of occurring to an eighty percent (80%) chance

of occurring in that resulting public sentiment derived from this occurrence will positively influence POST to mandate computer training to all new academy recruits.

The occurrence of Event 2 would have a minimal impact on Event 4 (legislation of funds for automation) by decreasing the probability from a forty percent (40%) chance of occurring to a thirty percent (30%) chance of occurring. Although there might only be one case, anti-law enforcement sentiment will be generated and thereby reduces the probability of legislation being enacted.

The event would have a moderate impact on Trend 1 (computerized law enforcement functions) decreasing the impact by two hundred percent (200%) to three hundred percent (300%) in that agencies that are automated may hesitate to expand until their security systems are validated as impregnable. Agencies that are not automated may hesitate due to the negative public sentiment generated.

The event would have a minimal impact on Trend 4 (information inundation) decreasing the impact by two hundred percent (200%) to three hundred percent (300%) overall, in that this type of case would generate some uncertainty about what types of information can be stored and retrieved.

The event would have a minimal negative impact on Trend 5 (big brother) by advancing the trends impact from two hundred percent (200%) to three hundred percent (300%)

overall. Again, an increase in this trend is seen as a negative reflection.

Event 3 - POST Mandated Training

Specifically, POST mandates that computer training be included as a performance objective in all police academies. If this event actually occurred, it would have a minimal impact on Event 1 (civil court case) by diminishing that probability from a fifty percent (50%) chance of occurring to a forty percent (40%) chance of occurring, as the number of computer trained law enforcement officers increases the chance of information being misused decreases.

The event would have a minimal impact on Event 2 (computer hacker arrested for piracy) by increasing in probability from a fifty percent (50%) chance of occurring to a sixty percent (60%) chance of occurring and Event 4 (legislation of funds for automation) by increasing in probability from a forty percent (40%) chance of occurring to a fifty percent (50%) chance of occurring in that increased computer training will slightly enhance the chance of a computer hacker being caught, and slightly influence the enactment of legislation.

The impact of this event is positive for those trends that are in direct relationship to the advancement of training. Trends 1 (computerized law enforcement functions), 2 (hardware technology - "dumb" terminal), 3 (software technology - artificial intelligence) & 4 (information

inundation) would experience an advancing of the impact by another two hundred percent (200%) as the use of the technologies will be enhanced by trained and experienced users.

Event 4 - Legislation of Funds for Automation:

Specifically, the Governor signs legislation which provides financial assistance or financial incentives for law enforcement agencies to automate.

If the State of California passes legislation which provides assistance to law enforcement agencies to automate all the other events would experience an advancement in probability.

If this event actually occurred then Event 1 (civil court case) will increase in probability from a fifty percent (50%) chance of occurring to a seventy percent (70%) chance of occurring, simply because the more agencies that automate, the greater the chance of misuse and subsequently the greater the chance of a civil case alleging abuse.

Event 2 (computer hacker arrested for piracy) would increase in probability from a fifty percent (50%) chance of occurring to a sixty percent (60%) chance of occurring in that there would be a larger pool of automated agencies for a hacker to infiltrate.

Event 3 (POST-mandated training) would be significantly advanced in probability from a sixty percent (60%) chance of occurring to a one hundred twenty percent (120%) chance of

occurring, because the demand for training would become inevitable and POST would respond accordingly.

Event 5 (language generated system offered at discount) will increase in probability from a sixty percent (60%) chance of occurring to an eighty percent (80%) chance of occurring, in that there would be a greater demand for development of this technology.

The occurrence of this trend would advance the impact of Trends 1 (computerized law enforcement functions), 2 (hardware technology - "dumb" terminal), 3 (software technology - artificial intelligence) & 4 (information inundation) because they would all benefit from a more competitive market as a result of the expansion of users.

Trend 1 (computerized law enforcement functions) is projected to experience an increase in impact by two hundred percent (200%) to seven hundred percent (700%) as the more agencies that automate the greater the vendor competition, thus, the greater the marketed capabilities available for all agencies.

Trend 2 and Trend 3 are impacted commensurate to the incentive perceived by the respective vendors. Again, the greater the market the greater the incentive. Trend 2 (hardware technology - "dumb terminal") is projected to increase in impact from six hundred percent (600%) to nine hundred percent (900%) and Trend 3 (software technology - artificial intelligence) is projected to increase in impact

from eight hundred percent (800%) to eleven hundred percent (1100%).

Trend 4 (information inundation) is projected to accelerate by five hundred percent (500%) to one thousand percent (1000%) because of the enhanced capabilities of newly automated agencies processing information efficiently and accurately.

Event 5 - Language Generated System Offered at Discount
Specifically, a software vendor "perfects" a voice activated portable unit and offers same to municipal governments at a substantial discount.

If this technology is improved and made affordable to law enforcement agencies it would exponentially increase their informational processing capabilities.

If this event actually occurred then Event 1 (civil court case) would experience an increase in probability from a fifty percent (50%) chance of occurring to a sixty percent (60%) chance of occurring, in that the greater the capability, the greater the use and subsequently the greater the chance of abuse. Therefore, the greater the chance of a civil law suit.

Event 3 (POST-mandated training) would experience an increase in the probability from a sixty percent (60%) chance of occurring to a one hundred percent (100%) chance of occurring, in that numerous computerized law enforcement functions would be substantially enhanced (i.e. computer

based instruction) and subsequently necessitate the need for a training process to start on the academy level.

Event 4 (legislation of funds for automation) will increase in probability from a forty percent (40%) chance of occurring to a sixty percent (60%) chance of occurring in that the advantages of this technology would be substantial enough to spark legislative attention to assist agencies who have as yet been unable to afford to automate their respective manual information processing functions.

This event would have significant advancing impacts on Trends 1 (computerized law enforcement functions), 2 (hardware technology - "dumb" terminal), 3 (software technology - artificial intelligence) & 4 (information inundation).

Trend 1 (computerized law enforcement functions) is projected to experience an increase in impact by three hundred percent (300%) to eight hundred percent (800%) in that the enhancement of this new technology would substantially improve the processing of information and the efficiency of the users.

Trend 2 (hardware technology - "dumb" terminal) is projected to experience an increase in impact by three hundred percent (300%) to eight hundred percent (800%) and Trend 3 (software technology - artificial intelligence) is projected to experience an increase in impact by three hundred percent (300%) to eleven hundred percent (1100%) in

that both of these trends are directly benefited by this technological advancement.

Trend 4 (information inundation) is projected to experience a substantial increase in impact by five hundred percent (500%) to one thousand percent (1000%) in that the enhancement of this technology would substantially improve the processing of information and the efficiency of the users.

FUTURE SCENARIOS

SCENARIO DEVELOPMENT

Scenarios are integrated mechanisms designed to bring together and synthesize large quantities of both hard and soft data that can not be handled systematically by any other means. The purpose of scenarios is to present alternatives or choices for strategic planners.

Basically a scenario can be in one of three modes:

- 1) Exploratory
 - play out
 - surprise free
- 2) Normative
 - favored and attainable
 - feared but possible
- 3) Hypothetical
 - worst case
 - best case
 - odd case
 - random case

Accordingly three separate scenarios have been developed based on the analysis of the NGT group on the trends and events and on the cross-impact analysis. The scenario modes used to depict the issues are;

- 1) Hypothetical - The "Big" One (worst case)
- 2) Normative - Hurricane Holly (best case)
- 3) Exploratory - High Tech Will Touch (most likely)

All three are driving force type scenarios.

Forecast Scenario #1: The Big One

Officer Carmen Martinez shook her head in disbelief as she surveyed the disastrous results of last night's earthquake. She reflected back to her grammar school days when she first started hearing about "the big one". How ironic, she thought, that on December 7, 1995, exactly 54 years since the Pearl Harbor attack, Americans are again experiencing devastating destruction. This time the enemy is unseen.

Carmen sifts through the rubble of her condominium until she locates her portable radio. She feels fortunate her radio will relay her communication via satellite, all radio towers are surely down today. To her dismay, she finds the radio frequency has been intercepted by organized crime figures who are transmitting narcotics pick-up instructions.

Carmen continues searching the remains of her home and finds her portable computer (an LD1 Unit). She attempts to contact her station by this means and is relieved when she gets a response. Through LD1, which is only the size of a brick, she immediately enters a report outlining the status of her beat. Carmen is a permanent resident of the beat she's assigned to patrol. She receives verbal instructions through LD1 to begin a systematic area search for injuries and fatalities.

Due to the LD1 unit Carmen continually communicates with, many people are reluctant to assist her by providing

their identification. Being unable to determine people's true identity makes it difficult to identify the fatalities and to account for the missing.

As Carmen continues her physical count, she also builds a business index. The index lists stores which are damaged, but securable; and those damaged, but unsecurable. The pattern of reports of looting at stores she has entered as unsecurable alerts her to the possibility of airwave piracy. Her mainframe's security audit is activated, and one unit on-line does not respond during this silent test. Security has been breached, a hacker has accessed the computer's data base.

Carmen attempts to use the alternate data transmission system (a back-up utilizing a cellular network) only to find it has been disabled by the earthquake.

Returning to LD1's main frequency Carmen tries to access the Artificial Intelligence mode to simulate this disaster for direction on alternative methods to locate the hacker.

Artificial Intelligence has also been disabled. Only basic emergency communication is possible now. While considering her next course of action, LD1 signals Carmen that a message is waiting. She reads "Catch me if you can" and a quick check of her sender codes indicates communication from an outlaw terminal - no sign-on for identification through the mainframe.

Carmen's frustration mounts as she realizes the hacker is taunting her. She is unable to close in on this phantom.

Then, Carmen is awakened to a DJ's voice announcing a "blast from the past", a 1987 hit "Who's That Girl." Carmen realizes she was only dreaming and is greatly relieved. Her relief is followed by amusement as she realizes that today is the day she's assigned to attend the Emergency Preparedness Planning Meeting. She verbally commands her in-house computer to turn on the TV and start the coffee while she heads for the shower.

Forecast Scenario #2: Hurricane Holly

Commander Kirk just completed his morning isometric exercises and now mounts his lifecycle for aerobics. He places his headset over his ears to listen to classical music. However, the music is replete with subliminal messages focusing on mental well-being.

Only two years ago Commander Kirk faced a stress retirement due to his ulcers and persistent migraines. As he reflected on the change in his health, he remembers his initial resistance and wonders why he was so committed to such poor habits.

At the completion of his aerobic exercise he inserts his right index finger into his pulse meter and is satisfied with the new level of his readings. After a quick shower, Kirk consults his nutro-computer readout for a listing of

breakfast options that conform to today's nutritional requirements for calorie, carbohydrate and protein content.

During his breakfast, he verbally commands the TV to play the morning news. News flash, January 2, 1995: "Court awards in favor of ACLU - Urban Police Department to pay 3 million in general damages, Chief Motoyama ordered to pay \$250,000 in punitive damages." The story then explained how ACLU's Chief Legislative Council Linda Feinstein was obviously pleased with this judgement as she was quoted saying, "This case demonstrates that one automated file on its own may not be abusive, but with the police philosophy of adding file after file a phenomena occurs. The totality of this phenomena has a frightening end result which no one can actually visualize, but it never the less impacts each one of us."

Kirk thinks to himself how relieved that chief must be to be part of the region-wide self-insured liability pool. This will pay most of his punitive damages and all of the general damages if the case is upheld on appeal.

Kirk gets in his car and verbally activates his mobile digital terminal.

Kirk, "Computer, this is Commander Kirk."

Computer, "Good morning, Commander Kirk."

Kirk, "Report on all major criminal activity in the past 16 hours."

Computer, "Please place palm on sensor for identity confirmation. Identity confirmed, thank you."

Case 95-0000134, double homicide occurred at Motor Lodge Inn. Within 3 hours, 2 suspects are in custody after computerized identification is made by the fingerprints left at the scene.

Case 95-0000212, child molest at New Hope Park. Victim and key witness provide a detailed verbal description. This is entered for a computerized composite and is circulated to all officers. Mainframe unit identifies suspect from composite scan and matches to confirm suspect's identity.

Case 95-0000301, armed robbery at Farmers and Merchants Bank. Three suspects were taken into custody as the result of a helicopter tracking their vehicle utilizing the electronic tracking system. (Suspects discarded 2 packets of money containing sensors, but missed a third packet.) Although momentarily thrown off track, the suspects were eventually located via the remote tracking receivers.

Case 95-0000427, grand theft at Merrill-Lynch. White male suspect described as "typical 3-piece business suit" type has apparently devised a method of branding stock certificates utilizing laser technology. The phony certificates could not be distinguished from authentic ones. Estimated loss: \$700,000.

Kirk, "Computer, give me the status reports on manpower deployment."

Watch Commanders

Lieutenant Bob Jenkins

Lieutenant Christine Marsters

Day Shift Field Supervisors

Sergeant Dok Hong

Sergeant Susan Kilday

Sergeant Judy O'Neill

Officer Deployment

9 field officers

1 K-9 unit

4 motor officers

2 computer technicians

6 community service officers

Vehicle Maintenance

Total miles logged last 24 hours - 2,664

Total fuel consumed - 66.6 gallons

Average MPG - 40

Financial Status

All departments are currently operating within budget

Weather Report

Clear and cold, high today 36 degrees farenheit

Low tonight 22 degrees farenheit.

Computer, "Will there be anything else, Commander Kirk?"

Kirk, "Yes, advise my secretary that I won't be in the office until 10:30. I will be at the police academy."

Computer, "Yes Commander Kirk, anything else?"

Kirk, "That will be all."

Computer, "Yes Commander Kirk, sign off 0828 hours, January 2, 1995."

Although Commander Kirk has had his language identification generation system (Ligs) in his car for almost three years, he still shudders to think he's holding a two way conversation with a computer.

Suddenly his thought is interrupted by an emergency on the radio - beep beep beep.

One Adam Twelve. One Adam Twelve. Bar scan of license plate in front of you reveals registered owner is Ralph Owens who has recently been identified as child molest suspect, Case #95-212.

One Adam Twelve, 10-4. Who's my backup?

One King 4 is eight blocks away to the east of you on Wilson Boulevard.

One Adam Twelve, 10-4

One King 4 copy, enroute.

Commander Kirk instinctively accelerates his vehicle and heads towards the pending felony car stop.

One King 4 to One Adam Twelve, I'm right behind you.

One Adam Twelve, 10-4. I'm going to activate VDU (vehicle disengagement unit).

The vehicle's engine is disengaged and the driver slowly pulls over to the right. The officers initiate a felony car stop but the suspect takes off running. Officer Kip Yee aims his laser unit and hits the suspect with a disabling electrical impulse and the suspect falls to the ground, unhurt, but unable to move. The officers handcuff the suspect and walk him back to their units. The suspect is still dazed but will fully recover in approximately 20 minutes.

Commander Kirk pulls up as the officers are placing the suspect in a patrol unit. Both officers smile as they spot the commander and neither are surprised. The technologies they used in this arrest were the result of a futures forecast initiated by Commander Kirk. The commander congratulates the officers for a job well done and then heads for the police academy.

At the academy he meets with the training coordinator and two representatives from POST. There are two topics on the agenda:

- 1) Governor Martha Wilson recently signed into law AB1303 which provides state assistance for police agencies to automate and financial incentives to police agencies who are automated but need to upgrade.
- 2) Effective January 1, 1995 POST mandated that all California police academies will include performance

objectives that encompass a minimum of 300 hours of computer training.

Neither of these major events happened by chance. Rather they were the result of an extensive cooperative effort of a unique collection of statewide law enforcement executives who are all members of CCAA (Command College Alumni Association). CCAA has become a powerful lobbying force at the state capitol as a result of their research into future issues that may effect law enforcement. The strategic planning and management techniques they have learned have served them well. Their charter is based on a concept taught by Dr. William Tafoya - that is - if policing is to influence its own destiny, law enforcement executives must chart the future course of action now. Thus far they have been adequately prepared for the "critical mass" that have opposed their efforts.

At the completion of this meeting, Commander Kirk finally heads for the office. Once at the office, Commander Kirk stops at the department's indoor range. There he observed officers using laser fitted handguns to enhance their simulated firearms training. (These weapons emit a pulse of light instead of a bullet.)

Commander Kirk glanced at his watch and saw that it was almost time for his teleconferencing meeting so he quickly walked up to his office. Commander Kirk was recently appointed to an international panel of police experts who

participate in weekly discussions that are made possible through satellite-transmitted television broadcasts. This week's panel discussion was on tactics and techniques that might be useful to combat the rising incidence of terrorism occurring on a world wide basis.

At the conclusion of the panel discussion Commander Kirk spent the next three hours working with the department's knowledge-based system. He spent the afternoon simulating different scenarios which depicted natural disasters, terrorist acts, monetary disasters, system security, and privacy invasion issues. The computer provided several alternative approaches for each scenario. These alternatives stimulated the Commander's thinking on each issue and assisted him as he began formulating pro-active policies that would assist the department in addressing these issues.

After completing this training experiment, Kirk now heads for home. As he is leaving the department he is greeted by an obviously excited Captain who informs him of how Hurricane Holly, the agency's expert system, helped defuse a volatile hostage situation that happened New Year's Eve. The Captain explains that after feeding Holly all the available data, the system found a correlation from the suspect's criminal history file and the suspect's psychological profile that indicated the suspect might be influenced by delusions of an alien from another planet, as past history includes alien encounters. Using a little old

fashioned human ingenuity, they dressed up a SWAT (Special Weapons and Tactics) officer in what they perceived a space alien might look like. Hurricane Holly then briefed this officer with some background data on scientific inter-planetary travel. The SWAT officer then made contact with the suspect who was completely in a trance when he saw the alien and easily disarmed. I imagine that without Hurricane Holly we would still be negotiating with that lunatic who, given enough time, would have undoubtedly hurt one of the hostages.

Commander Kirk was impressed with this operation, but was concerned that the case was not reported to him this morning by the computer. He mentioned this to the Captain who later reported there was a bug in the system and it has been corrected. Upon hearing this Commander Kirk thought that with all the technological improvements they've made, some things never change.

Forecast Scenario #3: High Tech Will Touch

Sergeant Wilson drove his patrol unit out of the back parking lot and was surprised to see the streets were wet with a light mist. Earlier he had been reflecting on the verbal reprimand he had just issued to Officer Robert Thompson.

Bob is a 24 year veteran and the epitomy of the old guard. He lives in the past and refuses to use his portable terminal in all but the most routine of tasks. Sergeant

Wilson should have spoke to him months ago, but Bob will be retiring next month with 25 years of service.

Next month thought Sergeant Wilson. Hard to believe it will soon be 1995. That is depressing, but what is even more depressing is the department will still have several "old guards" on board. If only the department's administration had involved the line officer in the pre-planning stages before automation. Then the resentment wouldn't have been as high and the officers would have more readily accepted automation given the opportunity for input. Yes, it's true, the days of tracking and processing multitudes of paperwork are long gone. Officers now use voice activated computers to dictate crime reports and car terminals to access a large information network. However all is not rosy. There are fewer officers on the street per capita as compared to 1985. This has necessitated that local police departments rely heavily on computer technology to assist in the efficient and expeditious processing of calls for service. In a day of high-tech high-touch, citizens are still demanding personal contact from police officers.

As Sergeant Wilson slowly rolls down the quiet downtown business section he contemplates the current state of affairs. Computer crime is now a major concern to law enforcement and will soon pass violent crime and property crime as the number one crime in UCR reporting. A mafia informant has recently revealed that organized crime has

developed an automated information network that equals or exceeds any state or local law enforcement's information system. Because prostitution and gambling have been legalized, organized crime is now focusing on the pirating of information. Technology is also benefiting the underworld in the manufacturing, distribution and sale of drugs. The advancements in designer drugs are proving to be a devastating influence on our youth. The advent of computer technology has had a major impact on the country's work force.

Seventy-five percent (75%) of the American labor force have jobs creating, processing, or distributing information.

By 1995 goods producing jobs will be at an all time low of twenty-three percent (23%), while service sector jobs will have risen to seventy-six percent (76%). By 1995 the work week has been reduced to 36 hours and between two fifths and three fifths of all workers are permanent part time employees. Twenty-five percent (25%) of all Americans are on flextime, and twenty-eight percent (28%) of all American workers are either sharing their jobs or working part time. By 1995 45-55% of all American workers will be using electronic terminals daily*.

*(Data on the American workforce was extrapolated and moderately increased from predictions made in a book by Jamieson, O'Mara, Soroken on "Managing the Changing Workforce". The book has not been released for publication yet and focuses primarily on projections for the year 1990.)

Recruitment and training of the 1990's police officer has been impacted by the advancement in technology. The Governor has a legislative bill on his desk that would provide financial assistance to all California Police Agencies to automate or expand existing systems. If approved funds will be collected from fines and criminal penalties and distributed to agencies commensurate with their crime rate and population served.

In 1988 Los Angeles County Sheriff's Department Police Academy was the first to offer computer training. Now POST has mandated that all police academies include one hundred hours of computer training. In addition, a majority of police academies are using the technologies of computer based instruction to teach the required performance objectives. Recruits that are using microcomputers in the learning experience have scored significantly higher on achievement tests. Citizens are now debating whether technology will serve the forces of expanding freedom or the forces of enlarging repression.

However as the debate forges on, a key element in this country once again surfaces; responsiveness. Citizens have learned that if they fail to be part of the solution, then they are part of the problem.

Task forces have been formulated to identify public safety issues and develop plans of attack. Citizens are volunteering to use their home computers which can be linked

to the departments to assist in the high demand for data entry. Computers are also used for crime prevention programs such as neighborhood watch to assist in the dissemination of information. It is now a requirement that at least one member of a neighborhood watch program have a home computer. It is not uncommon to see community fund raising projects to assist those in need. This is demonstrated by reference to a recent article in USA Today.

High Tech Will Touch

In Lodi, California a new version of Saturday Night Bingo surfaced last night. Members of SIL-ALI (Stuck In Lodi - And Loving It) held their first annual fund raising event. The purpose of this event was to provide an opportunity for all neighborhood watch programs to have at least one computer terminal in their group. With a new twist in bingo, giant bingo cards were outlined on the floor of the community center. Eligible neighborhood watch groups had members stand on the numbers as they were called. The excitement was contagious as the groups yelled different chants of support for their members. The winners each received a home computer and a commitment from trained volunteers to assist a designated member with hands on experience. Local merchants and civic groups donated the computer terminals. Nancy Chinn, a grateful winner, expressed her pleasure by quoting from the ageless song, "we are the world, we are the ones who make a better day."

Sergeant Wilson glanced at his watch and was surprised to see that his shift was almost over. As he headed back to the station his thoughts turned to the all expenses paid annual fishing trip he and his fellow Sergeants were awarded this year for a job well done.

At this point trends have been examined and events considered. The cross-impact analysis is complete and relevant scenarios were extracted from the insight of combining these endeavors. All the forgone efforts point to now examining a strategic plan which can most efficiently accomplish the desired objective, the effective managerial use of automated police data.

OBJECTIVE TWO

OBJECTIVE TWO

STRATEGIC PLAN

Statement

The second objective is to develop and implement a strategic management process to include:

- o Strategic Decision Making
- o Strategic Planning
- o Policy Considerations

Because strategic planning is not linear the above three items are interactive in the process. The anticipated outcome of this process is a strategic plan, bridging the gap between the present and the scenario-based future.

METHODS IDENTIFICATION

In the development of the plan the following methods were used:

- o SMEAC Model
 - Situation
 - Mission
 - Execution
 - Aministrative
 - Control
- o Capability Analysis Model
- o Stakeholder Identification and Analysis
- o SAST
- o WOTS-Up Analysis
- o Modified Delphi Policy Analysis

METHODS IMPLEMENTATION

Situation

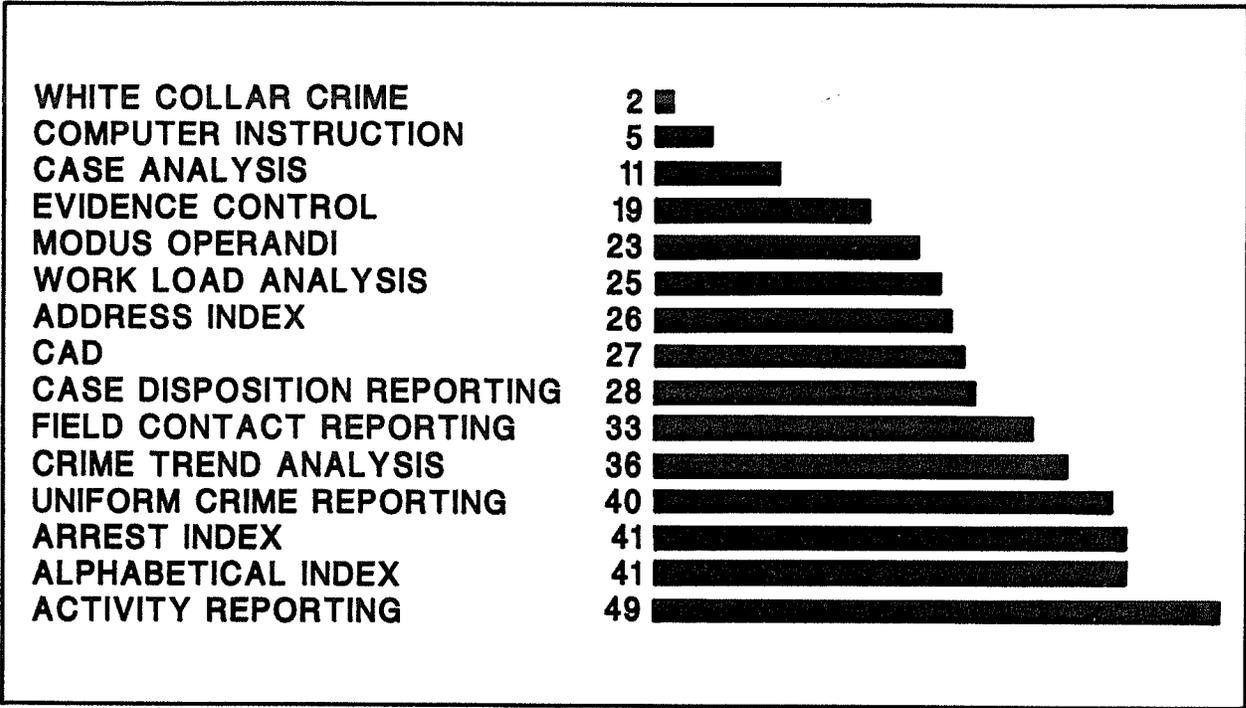
Environment

During the mid-1970s it became increasingly apparent that technological developments in the computer industry and the application of automated data processing to law enforcement agencies were having significant impact on the management and operation of many agencies(17). However, as we're approaching the end of the eighties only about 1/3 of California's police agencies have some form of computerization. The majority of police agencies in California that are not automated are the smaller departments. For California's law enforcement agencies serving a population of 100,000 or more, 41 out of 50 (81%) have some form of automated crime information system. (According to a recent survey conducted by DOJ; refer to interview of David Roberts.)

In 1976 Search established the National Clearinghouse for Criminal Justice Information Systems to promote and facilitate the transfer of proven criminal justice information systems. In support of this purpose the Clearinghouse created a computerized index of justice systems, the Automated Index of Criminal Justice Information Systems. The index is continually updated through surveys and agency contacts on a nationwide basis. Search believes that this index is the most up-to-date information available

on operational and developing criminal justice information systems nationwide. The index data base is used to generate the contents of the Directory of Automated Criminal Justice Information Systems. There are 17,000+ law enforcement agencies in the nation and this index has a listing of approximately 1,000 agencies that have some form of automation. This listing is not inclusive and there are undoubtedly a number of law enforcement agencies who have automated but are not included in this index.

From the agencies that did respond to surveys and contacts from Search, the following information can be gleaned.



THE NUMERICAL NUMBER REPRESENTS THE NUMBER OF CALIFORNIA AGENCIES REPORTING A SPECIFIC CAPABILITY. IT SHOULD BE NOTED THAT SOME OF THE AGENCIES COULD HAVE ALL OF THE CAPABILITIES.

What is depicted by Search is admittedly not a complete picture as all agencies have not reported their systems to the Search Group. For example, without knowing how many California law enforcement agencies responded to the Search inquiries, you can take any of the given categories listed in the chart and triple the number of agencies and it would still fall below 1/3 (33%) of California's 475 police agencies that are reporting automation capabilities. The chart also supports an IACP staff analyst conclusion that only 10% of the police departments that have computers use them in imaginative ways(18).

It should be obvious to all that the piece of equipment and associated technology that will have the greatest impact over the next few years is already here. The computer is becoming a major factor and as it continues to be refined and upgraded, it will become the most dominant factor in policing since the patrol car(19).

Law enforcement historically has not seen itself as a business. But law enforcement is exactly a business. We produce a product and supply a service. Our product is a safe community, or if we are faulty in our production, perhaps an unsafe community. Our service is the apprehension of those who threaten another's safety, or who threaten their own. Law enforcement's reluctance to see itself as a business has translated into underuse of technologies which enhance the business process.

Such has been the slow acceptance of computer use in law enforcement. This tool, the computer, has greatly impacted the manner in which many agencies do business. For years, the private sector business world was utilizing this tool. Rather recently, law enforcement has embraced the capabilities of this tool and in so doing has the potential of maximizing the effectiveness of its business.

At issue then, is the degree to which law enforcement makes use of present generation computers and state of the art technology(20).

It seems reasonable to assume that if local law enforcement is not now using computers innovatively, it is a reflection on the capabilities of the personnel responsible for operating such technology(21). We will be compelled to endure the future if we do not shape its course(22).

In order to bridge the gap between the environment depicted in this monograph and the future depicted in the normative (best case) scenario, the following analyses are presented. This process should facilitate a better understanding of how law enforcement can develop techniques to bring about a desired future state.

Policy Considerations

The scenarios depicted in the first objective demonstrate that police executive management capabilities will change substantially with the advent of computers and advanced technologies intrinsic to automation. It is difficult to predict whether using computer technologies to advance management capabilities will be realized. The extent to which computer technology can be applied to law enforcement's management capabilities seem almost infinite. However, law enforcement is far from realizing potential management enhancements afforded by computers.

To facilitate a positive atmosphere for law enforcement management to realize the greatest potential the following policies are submitted for consideration:

- 1) Law enforcement should promote an affiliation with computer experts in the private sector.
- 2) One of the already established law enforcement affiliation groups (i.e. CPOA, IACP) should be encouraged to actively lobby state and/or federal sources for funding to facilitate technological enhancements.
- 3) Law enforcement needs to be intuned to the financial impact of computerization with enhancements and prepare accordingly.
- 4) Law enforcement managers should utilize user participation, possibly in the form of steering committees, to ease the assimilation of change within the organization.
- 5) Law enforcement should actively seek any available training in automation to increase the degree of computer literacy in management.
- 6) Law enforcement should actively encourage POST to increase the level of trianing presently offered and to include hands on computer training as a performance objective in police academies.

Stakeholder Identification & Analysis

Stakeholders are any vester person or group whose behavior is affected or whose behavior in turn effects the issue. Among stakeholders is a sub-culture known as

snaildarters, an individual or group that blocks or thwarts the direction of the organization. Stakeholders and/or snaildarters can be internal or external to the organization, and their efforts to support or oppose can be overt or covert. Stakeholders and snaildarters can be counted on to have one or more opinions about the impact that a new direction, strategy, or program will have on the issue. An organization formulating any strategic plan must identify the individuals or groups and have a clear understanding of their opinions and/or assumptions. This is a critical aspect of the strategic planning process.

During the NGT workshop the group brainstormed a list of stakeholders and snaildarters. Out of this list of thirty-six (Appendix I) a consensus was obtained and the list was distilled to the seventeen considered critical to the main issue of this monograph: police executives managing with computers... Each of these stakeholders can impact/affect, policy or goals within an organization. Evaluating and plotting their positions is an important tool.

The following is a list of perceived assumptions of the most significant stakeholders/snaildarters to the issue:

1. Sworn Personnel
 - a. may overtly or covertly oppose computerization wanting to protect the status quo/old guard

- b. many consider managements automated manpower deployment capabilities as an internal big brother issue
- c. will sense the necessity to become computer literate
- d. will show greater efficiency in the report writing process
- e. may fear loss of promotions due to potential reduction in middle management positions
- f. will have greater access to more comprehensive information at the line level
- g. might enjoy more esteem through association with progressive department

2. Non-Sworn Personnel

- a. will fear work force reduction
- b. will become bored with mundane data entry tasks
- c. might resent status and prestige of sworn personnel
- d. will feel pressure from the big brother syndrome about accuracy of information
- e. will fear a depersonalized work place due to technology enhancements

3. Sworn Management

- a. will be concerned about lawsuits over misuse of information
- b. will embrace the capabilities automation will afford them for administrative control

- c. may fear loss of promotions over concern of reduction in middle management positions due to automation
- d. concerned about hackers accessing and pirating information
- e. fear of the unknown, thus slow to interact with new technology

4. Non-Sworn Management

- a. will be concerned about lawsuits over misuse of information
- b. will be charged with responsibility of insuring accuracy and efficiency of civilian personnel
- c. will embrace the capabilities automation will afford them for administrative control
- d. concerned about hackers accessing and pirating information
- e. may experience philisophical differences between civilian managers and sworn users

5. Taxpayer

- a. concerned about increased budgets for municipal governments
- b. demand same level of service but expect no increase in costs
- c. resist any attempts to increase taxes
- d. demonstrate mixed support for an agency's acquisition of federal or state funding

- e. could be apathetic towards law enforcement's use of technologies
6. Media
- a. understands advent of computer technology
 - b. always concerned about big brother issues
 - c. any sensationalism (positive or negative) will be exposed
 - d. cultivate media for public education efforts
7. Police Associations (Unions)
- a. quick to deal with internal big brother issues
 - b. concerned with protecting status quo
 - c. may sense more emphasis on technology and less on human aspects of job
 - d. view computer technology as a means to reduce manpower
8. Organized Labor Unions (i.e., Teamsters)
- a. concerned about competition for jobs
 - b. concerned about potential loss of jobs
 - c. concerned about technological expertise which might be expected from veteran employees
 - d. cost of equipment impact on salary/benefit increases
9. Groups Concerned with Civil Liberties
- a. will demand accuracy of information
 - b. will quickly challenge misuse of information
 - c. will constantly focus on big brother issues
 - d. will resist statewide or national networking efforts

- e. will be concerned about cross-indexing of different files

10. Hardware/Software Vendors

- a. will continue to develop new systems commensurate with public sector funding
- b. will strive to provide viable products that are affordable for the majority of agencies
- c. will push forward with new technologies
- d. will offer discounts to state and local governments
- e. may misunderstand law enforcement's functions and programs may not address management needs

11. Seniors

- a. will constitute a larger percentage of the population between 1990 and 2000
- b. any efforts at passing bonds or special tax assessments will have to gain seniors support
- c. seniors living on fixed incomes will have greater demands for cost efficient municipal services
- d. seniors are normally supportive and appreciative of law enforcement efforts to develop effective crime fighting strategies

12. Local Politicians (City Council/Board of Supervisors)

- a. concerned about costs of automation
- b. concerned about abuse of information
- c. concerned about civil lawsuits

- d. must deal with pressure from other city departments over allocation of shrinking financial resources
- e. lack of understanding over law enforcement's use of information system

13. State and Federal Politicians

- a. will continue to monitor privacy issues
- b. funding priorities in constant state of flux
- c. will probably resist nationwide law enforcement information network
- d. may experience pressure from constituents concerned about crime, thus more prone to dialogue with law enforcement

14. Judges/Courts

- a. constantly asked to evaluate legalities of new technologies
- b. will be familiar with computer technologies from personal experience within their arena
- c. will be asked to evaluate how computer technology supports or opposes individual(s) constitutional rights
- d. concerned with big brother and privacy issues

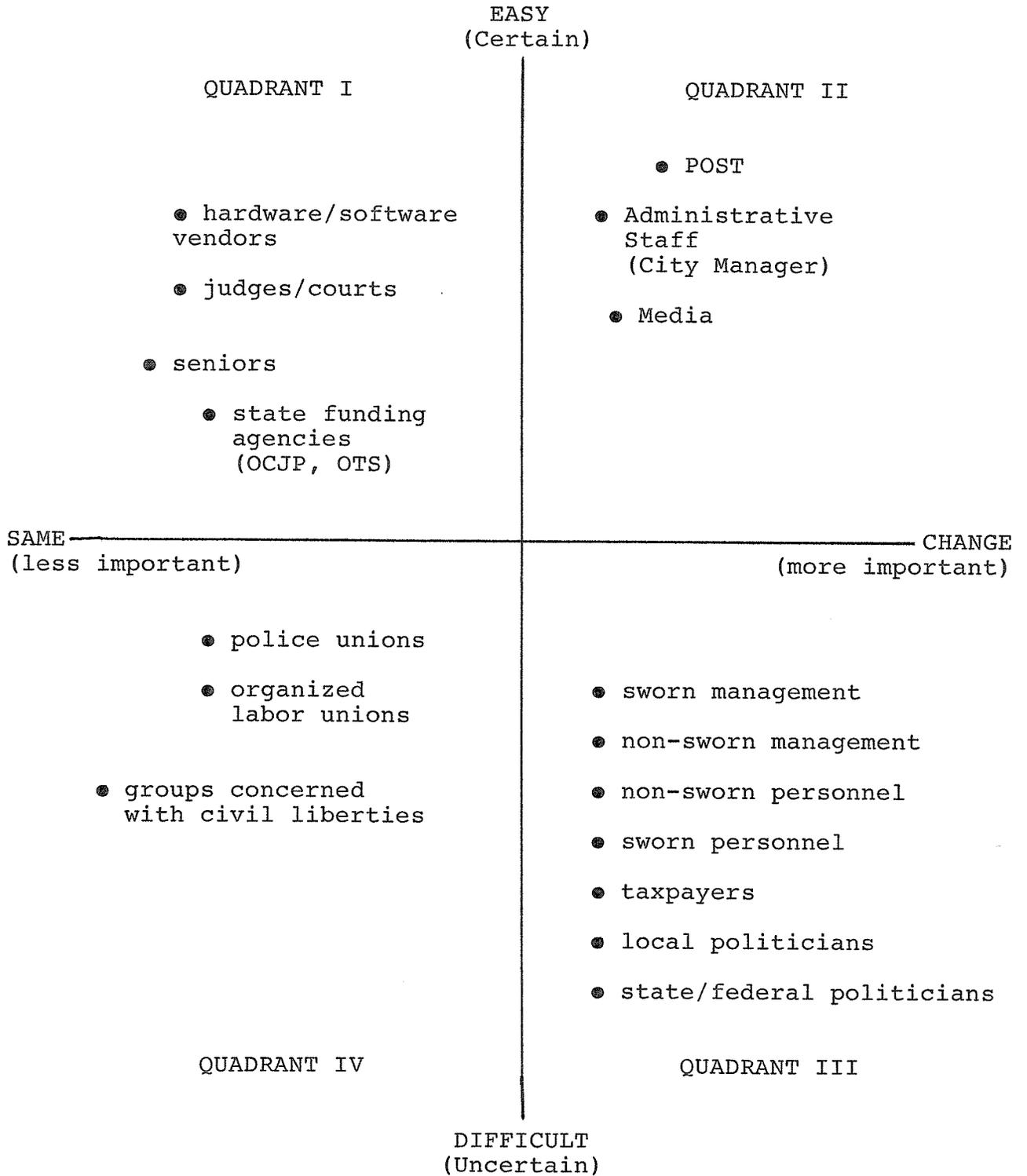
15. State Funding Agencies (i.e., OCJP, OTS)

- a. will provide funding for agencies to automate as they address specific criminal issues

- b. will experience increased competition for state and federal funds commensurate with the shrinking of municipal government's financial resources
 - c. will financially support and subsequently foster innovative computerized functions/concepts
16. Administrative Staff (City Manager/County Administrator)
- a. establish policy and control of automation process
 - b. concerned about civil lawsuit potential from misuse of information
 - c. will probably understand the multifacet advantages of computerization
 - d. concerned about the financial impact
 - e. attuned to citizen's concerns about automation issues
17. Commission on Peace Officer Standards and Training (POST)
- a. might be the impetus to induce legislators to provide funding to law enforcement agencies to computerize their various functions
 - b. will have to consider mandating police academy performance objectives that focus on computer training for new recruits
 - c. will train law enforcement administrators on civil liability issues concerning misuse of information

The following graph is the writer's assessment showing the stakeholder's position to the ease or difficulty that will be encountered in obtaining their support.

STAKEHOLDER EVOLUTION



WOTS-Up Analysis

The WOTS-up acronym is an analysis of an organization's weaknesses, opportunities, threats and strengths that must be dealt with internally (in this case the organization is law enforcement as a whole).

The WOTS-up analysis is designed to aid a strategist in finding the best match between the internal capabilities within any organization that will impact the issue. Specifically in this case - Police Executives Managing With Computers . . . Where Will We Be In 1995.

Definition of Terms

Opportunities - Any favorable situation

Threats - any unfavorable situation

Strengths - A resource or capacity used to achieve objectives

Weaknesses - limitations, faults or defects

Opportunities

- o artificial intelligence
- o portable lap computers
- o portable dumb terminals
- o cost of computer hardware and software are decreasing
- o software and hardware vendors are becoming very competitive
- o the competitiveness will lead to exciting computerized innovations which will enhance law enforcement's capabilities
- o computer navigation
- o capabilities of laser technologies
- o electronic tracking systems

Strengths

- o computers can generate investigative leads, manage cases, spot crime trends and forecast where criminal may strike next
- o CAD systems can prioritize calls, identify available units, track field units and alert dispatchers to officer safety issues
- o increase organizational accountability and efficiency
- o automative information systems provide quantitatively and qualitatively more information

Threats

- o ACLU through legislative lobbying challenging law enforcement information systems
- o budget restraints
- o shrinking fiscal resources
- o lawsuits which might curtail law enforcement's use of information systems
- o shrinking resource of qualified personnel
- o control over information has the potential to change the distribution of power within police agencies

Weaknesses

- o law enforcement is probably a decade behind private industry in terms of computerization
- o computer literacy among law enforcement personnel is low
- o law enforcement's reluctance to share information
- o poor hardware and software compatibility
- o law enforcement has been slow to utilize new technology
- o automation costs will consume a greater portion of an agency's resources
- o many law enforcement executives do not understand the issues of compatibility between hardware and software
- o most agencies using computer capability merely as electronic file cabinets

Resource Analysis

As we, who work in public entities, live in an era of shrinking financial resources, it is easy to be discouraged from attempting to automate or upgrade an existing system. Each law enforcement executive has to make an individual determination of the fiscal feasibility of automating a police agency or increasing the capabilities of an already existing system.

The writer has learned from personal experience that one does not just go out and buy a computer and transform an agency overnight. It must be understood that it doesn't take weeks, months, or even years to facilitate the entire process of computerization. It might take a decade or two, but no progress is stagnation.

"Necessity is the Mother of Invention" and law enforcement executives have been finding creative ways to finance an automation process within their organization. At the present time there are state funding agencies offering grants and computer vendors offering state and local discounts. One could make a good argument that now the time is right. Hardware and software vendors are keenly aware of the competitive atmosphere prevailing the law enforcement market arena. A law enforcement executive who is well prepared can take advantage of this most opportune time and obtain the hardware and software necessary commensurate to the size of the public entity represented.

When dealing with technologies one of the difficulties is insuring that short term decisions are consistent with long term goals. "Where there is a will there is a way." The capability for most law enforcement agencies to automate exists, one only has to find the way.

Human Resources

Training should be provided for management development at the same rate as technology's change.

Law enforcement managers should realize that change is not necessarily a problem, but often an opportunity - people that fail are those that react to change wrongly.

Automation by its own dynamic will mandate changes, what is not known is the extent of conflict and the cost such reforms will require. (23)

Another unknown is how effectively police administrators will use the information generated by automated management systems. Does it contribute to information overload? Are police managers sophisticated enough to take advantage of this tool? Will agencies reorganize and develop the administrative strata necessary for technical specialists to emerge? (24)

Will information specialization result in conflict between sworn personnel who claim the right to make decisions and specialists who claim the knowledge to make decisions? Answers to such questions remain elusive. (25)

An analysis of human and financial resources must take these issues into consideration.

Mission

In the simplest form the mission of any law enforcement agency is the prevention of crime.

In an effort to provide a framework for this strategic plan, the following mission statement is offered to help focus and define the main issue.

Mission Statement

To provide California law enforcement executives a model for dealing with crime incidents and management of information in a more efficient and expedient manner by:

- o seeking out new technologies
- o developing a high level of computer literacy
- o exploring new ways to harness computer capabilities
- o maximizing existing software programs
- o cooperating in the sharing of information both internal and external to the organization
- o networking whenever possible with other criminal justice entities

EXECUTION

Strategies

A modified Policy Delphi was used to address the issue of police executives managing with computers; in terms of the present environment and resources and to assure a well managed, objective driven guide to the future. Three

alternative courses of action are now advanced for consideration.

Alternative One

Contract with a private consultant to evaluate an agency's existing system or to conduct a needs assessment for an agency considering automation. The goal of this assessment would be to formulate policies and procedures that promote a steady but consistent assimilation of automation that includes specific focus on the management of the generated information.

PRO- Today the majority of police administrators are not computer literate whereas a private consultant would have the expertise necessary for such a formidable task as initiating or enhancing an automation process.

PRO- A private consultant with a holistic approach would be better equipped to formulate the necessary management prospective.

PRO- Use of an experienced consultant would probably expedite the assimilation process. As the old adage goes... why reinvent the wheel.

CON- The financial impact of hiring a consultant might be prohibitive to smaller agencies and restrictive to larger agencies.

CON- A private consultant may not understand the informal network within the organization or may have preconceived

solutions or inclinations that may not be acceptable to the organization.

CON- If a careful choice of the consultant is not made, the end result could be a digression rather than progression of the automation process. (The writer is familiar with organizations that used consultants that delayed by 2-3 years their development process.)

Alternative Two

Appoint an in-house executive task force, consisting of management staff, supervisors (sworn and non-sworn), line personnel (sworn and non-sworn), one or two members of a city data processing staff and two or three community members who are familiar with computer operations. This task force will develop policies and procedures that promote a steady consistent assimilation of an automation process with a specific focus on the management of the flow of information generated through computerization.

PRO- Facilitates a faster acceptance of an automation process generated by committee members sharing the new capabilities with fellow employees and subsequently averting a sabotage or rejection of new applications.

PRO- Generates a variety of different perspectives on how the flow of information should proceed within the organization and provides a means of receiving valuable input from those who will work with the system on a daily basis.

PRO- By employing this concept the department head demonstrates a commitment to actively pursue the automation process and the development of a system that works for the people.

CON- This concept might accentuate the bureaucratic process that already exists within an organization and subsequently impede the automation process.

CON- With a low degree of computer literacy within law enforcement, this concept runs the risk of vendors inducing acceptance of a system that may not meet the needs of the organization.

CON- Facilitation of a task force of this nature could be inherently difficult because of individual members striving for a competitive edge from the process of automation.

Alternative Three

Contract with a private computer firm to fully equip, monitor, maintain and manage an automation system within a law enforcement agency with the only cost to the city being an installment fee and monthly service fee.

PRO- Contracting with a private provider would reduce the number of public employees (permanent work force) and the costs associated; i.e. salaries, benefits and training.

PRO- Frees up management and supervisory time necessitated from an in-house development and operation plan needed to accomplish the same objective.

PRO- As in most privatization concepts, the amortization of costs are spread out among other agencies and subsequently less costly than in-house systems.

CON- Security of confidential records would be of paramount concern with this concept. The legalities would have to be explored very carefully.

CON- Civil liability issues are intrinsic to this concept in that agencies would be dependant upon a private firm for the validity of the information they deal with on a daily basis.

CON- The training time necessary for a private firm to understand all the intricacies of the criminal justice systems might be prohibitive.

Recommended Alternatives

An overall evaluation of the alternatives and their immediate and long-term potential impact in addressing the advent of police executives managing with computers a merging of alternative one and two was selected as the most feasible guide to the future.

There are two focuses of the main issue of this monograph: 1) the majority of law enforcement agencies in California and the nation are still not automated, and 2) the

majority of those agencies that are automated are using their systems for the most routine of tasks.

A combination of these two alternatives will assist law enforcement managers in the acquisition of a system that meets their needs, and/or the enhancement of an existing system if necessary. Also, the optimum use of computer technologies will improve the effectiveness of the organizations management.

A marriage between a consultant and an in-house task force provides the best of both opportunities. The complexity of computer technologies almost demands the services of an expert, especially to insure that the short term goals address the organization's long term needs. In addition, the use of the task force will tap the in-house expertise and promote a buy-in among the "users". It is also recommended that community members participate in the task force to promote support and defuse the big brother syndrome.

Administration and Logistics

The implementation of this strategic plan must be based on a foundation of mutual understanding between the consultant and the executive task force.

The short and long term impacts of automation and managing with computers must be clearly understood by all participants. The tendency is to move ahead to quickly with stop gap measures and then initiate a band aid approach when things go wrong.

Subsequently it is recommended that a deliberate and methodical approach be initiated that focuses on all the necessary elements of automation and management.

Funding and Logistics Implementation

- o Agencies that are initiating an automation system can use several approaches
 - 1) conduct on site visits with agencies that have already automated and begin to formulate the approach to be taken (3-6 months)
 - 2) consult with Search Group Inc. or IACP and receive direction on the available systems that might best meet the department's needs (3-6 months)
 - 3) consult with private consultant and have s/he make recommendations on the best system that will meet the department's needs (3-6 months)
 - 4) a combination of the above three approaches (6-12 months)
- o Conduct search for consultant
- o Estimates are normally free, so first get an idea of what a consultant will charge for his services. A bid process may be necessary. If the bid process will be bypassed, seek approval for a sole source agreement.
- o Prepare a presentation for the City Manager outlining the results of a needs assessment, the anticipated accomplishments, and costs of implementation (1-2 months)
- o Advanced plan to the City Council (1-2 months)

- 1) presented with a futures perspective
 - 2) presented with alternative funding if available
(i.e. state funding or civic group contributions
for smaller systems)
 - 3) outline the pros and cons of the selected
alternative
 - 4) request council approval of selected plan
- o Upon Council approval, establish time line for
accomplishment of specific objectives and initiate
process (6-9 months)
 - o Negotiate with selected stakeholders/snaildarters to
gain support for the plan (3-6 months)

For the purpose of this monograph, a generic approach was taken to the analysis of the most appropriate planning system to be introduced with the implementation of this strategic plan.

Looking at law enforcement as a whole analysis of the environmental turbulence indicates "many changes", that will occur when considering automation and/or management enhancements. Analysis of the predictability of the future when dealing with automation and/or management enhancements indicates predictable threats and opportunities as indicated through the WOTS-up analysis.

The following planning system matrix demonstrates these assessments and depicts the planning system identified to be

The periodic planning process is a proactive approach that aligns specifically with the selected alternative, coordinating the services of a consultant with an in-house executive task force, to advance the organization to the issue of managing with computers.

With the strategic plan analysis complete, this monograph will now focus on a plan to facilitate the transition.

OBJECTIVE THREE

OBJECTIVE THREE

Statement

The third objective of this monograph is to develop the transition process by which the plan developed in Objective II is strategically managed to produce the selected future scenario.

To further clarify this process the writer is drawing on the resource of a mid-size municipal police department, serving a residential community of 50,000. Community stakeholders felt to have a vested interest in managing with computers were identified and a mission statement was developed. With the present assessed, the future forecasted, environment defined, and resources identified, a Strategic Plan was developed to provide a guide for the future of managing with computers in the law enforcement arena. The focus of the transition plan is to facilitate an implementation process transcending from the present to the future.

Methods: Identification

- o Critical mass analysis
- o Readiness/capability charting
- o Implementation analysis

Methods: Implementation

Critical Mass

To improve the impact of police executives managing with

computers there are a number of constituencies (critical mass) whose involvement is necessary to create the best environment necessary for the changes to occur.

They are identified as follows:

- 1) Sworn Personnel
- 2) Non-Sworn Personnel
- 3) Sworn Management
- 4) Non-Sworn Management
- 5) Administrative Staff (City Manager
- 6) Media
- 7) Police Association
- 8) Local Politicians
- 9) State/Federal Politicians
- 10) Computer Vendors
- 11) POST
- 12) Civil Liberty Groups

Focusing on a mid-size law enforcement agency, a commitment analysis was completed. This enabled an assessment to ensure that the appropriate strategies were well defined for each member or group of the identified critical mass.

The below commitment analysis chart illustrates the perceived position and projected movement necessary by each stakeholder. The writer used his own organization to develop these perceptions.

COMMITMENT ANALYSIS

CRITICAL MASS PLAYER	BLOCK THE CHANGE	LET CHANGE HAPPEN	HELP CHANGE HAPPEN	MAKE CHANGE HAPPEN
SWORN PERSONNEL	X	→ O		
NON-SWORN PERSONNEL	X		→ O	
SWORN MANAGEMENT		X		→ O
NON-SWORN MANAGEMENT		X		→ O
ADMINISTRATIVE STAFF		X	→ O	
MEDIA		X	→ O	
POLICE ASSOCIATION	X	→ O		
LOCAL POLITICIANS	X	→ O		
STATE/FEDERAL POLITICIANS	X	→ O		
COMPUTER VENDORS			X	→ O
P.O.S.T.			X	→ O
CIVIL LIBERTY GROUPS	X	→ O		

X - PRESENT POSITION

O - DESIRED POSITION

Sworn and Non-Sworn Personnel - Typically line officers and their civilian counterparts will be resistive to automation and subsequent enhancements if for no other reason than the fear of change. The other perceived assumptions of stakeholders (outlined in the stakeholder analysis) will need to be addressed. This can best be accomplished by including them in the facilitation of the technologies. By being included, the stakeholder's collective experience becomes a valuable resource. Initially, these employees will block the change, but through their involvement movement can be expected. Sworn personnel can be convinced to let the change

happen and non-sworn personnel can be persuaded to help the change happen.

Sworn and Non-Sworn Managers - Typically police managers and their civilian counterparts will be willing to let change happen. Their participation in this particular process is seen as paramount to success. With the proper insight, managers will have a holistic perspective on how technologies can assist them and their organization.

Although concern may exist over potential lawsuits and reduction in middle management positions, these managers can generally be expected to strive for successful transition. For movement to occur from "let change happen" to "make change happen" the indoctrination process is seen as most critical.

Administrative Staff (City Manager) - A typical City Manager will be concerned about the financial impact of an automation program. The manager will also insure that short term decisions are consistent with long term goals. Because of his political influence he should be persuaded to help the change happen. He is seen as a critical factor in encouraging movement among local politicians.

Media - Most members of the media understand the advent of computer technology, and will normally be in the "let change happen" category. Because of their influence with most other stakeholders, the media should carefully be cultivated for support. They should be persuaded to help change happen.

Police Association - Management needs to thoroughly understand the fears that line officers may experience with the advent of computer technologies. Special emphasis should be placed on addressing those concerns and relieving their anxieties whenever possible. Their initial response will probably be to block the change overtly and covertly when possible. However, by dispelling their fears, they should move from "block the change" to "let it happen".

Local, State and Federal Politicians - Members of these groups can be of assistance or hindrance depending on how they are cultivated. A prevalent issue today is citizens concern about crime. Constituents will continue to keep politicians focused on the need for attention to this issue. By utilizing this, management can move politicians from "block change" to "let change happen".

Computer Vendors - Both hardware and software vendors are keenly in tune to the viable market presented by law enforcement. The competitiveness experienced by vendors will lend itself to the enhancement of management technologies. Through cultivation, vendors can be moved to "help change happen" to "make things happen" by the technologies they develop.

POST - Regarding the technology issues POST can be viewed as a trend setter. Their influence through Command College, Executive Development Courses, and a variety of management courses can be viewed as an avenue for influencing law

enforcement's embracement of computer technologies. With encouragement, they can be moved from "help change happen" to "make change happen".

Civil Liberty Groups - Members of this group are probably law enforcement's greatest critics. Movement from "block change" to "let change happen" may be difficult but not impossible. The issues of this group need to be clearly understood and addressed in an open, realistic manner. The group's concern about accuracy, privacy and misuse of information need to be dealt with. If law enforcement ignores these issues this group can become the classic snaildarter.

Readiness Capability Chart

This technique serves as a means of comparing members of the critical mass that are crucial to the change effort. Each member is then ranked according to their readiness with respect to the change.

READINESS/CAPABILITY CHART

Fill in the following chart as it applies to your situation. In the left-hand column, list the individuals or groups who are critical to your own change effort. Then rank each (high, medium, or low) according to their readiness and capability with respect to change.

	READINESS			CAPABILITY		
	High	Medium	Low	High	Medium	Low
1. sworn personnel			X		X	
2. non-sworn personnel			X		X	
3. sworn management		X		X		
4. non-sworn management		X			X	
5. administrative staff		X		X		
6. media	X			X		
7. police associations			X		X	
8. local politicians			X		X	
9. state/federal politicians			X		X	
10. computer vendors		X		X		
11. POST		X			X	
12. civil liberty groups		X			X	

Transition Plan

The alternative selected in Objective Two must be monitored to insure implementation. The implementation plan is a general framework for monitoring the complex activities associated with the strategic plan. The task force must have considerable latitude to determine the specific techniques to be utilized in accomplishing the stated objectives. Subsequently, detailed approaches have not been assigned. For the reader's consideration the following generic techniques are presented for consideration.

Force Field Analysis

In this technique members of the critical mass are plotted either as positive forces helping or negative forces hindering. A decision is then made as to how key players who are hindering your efforts are moved to the desired state.

It is recommended that tactics designed to accelerate the positive forces and to lessen the negative forces be identified and pursued.

Confrontation Meetings

This technique is often used in team building in an effort to surface hidden agenda's or negative feelings. Present values and roles are clarified and individual support is sought.

Activity or Process Plan

Critical incidents and specific activities that must occur are identified in this approach. This technique is cost effective and serves as a road map for change. Task, specific, purposeful, integrated, time-specific are samples of techniques that can be used.

The implementation plan is the means to insure success of the strategic plan. Given any type of plan, successful implementation is the key element. Lines of communication must be very clear, individual responsibilities must be understood and commensurate with the proper level of authority.

Through the methods used in this monograph the analysis shows the assimilation of automation will require a deliberate, methodical approach by managers who have authority to dictate policy.

The strategic planning process of this exercise surfaced relevant issues that cannot be ignored if one hopes for a successful transition. Some of those issues include:

- 1) support must begin at the top of the organization, but acceptance must be earned from the bottom up,
- 2) all participants must have a clear understanding of what the main objectives are and how the assimilation process affects them,

- 3) acknowledge that the fastest way to gain acceptance is to request participation and constructive criticism,
- 4) key personnel should responsibly orchestrate the automation process and not entertain unfocused diversity,
- 5) simply stated, the process won't happen overnight and should be directed along a realistic timeline.

CONCLUSION

CONCLUSION

If law enforcement executives are to manage rather than be managed they must meld their role into the technological advancements or be left behind. The ability to direct and accept the changes presented by computer technology may be the paramount challenge to managers in the 90's. To be inflexible, or strictly reactive, to opportunities to enhance management with automation could leave managers isolated in an outdated environment.

In Objective One, modified Delphi techniques were used to analyze what were considered relevant events and trends. Comparisons were made through cross-impact analysis which defined issues for consideration in the scenarios.

To manage such a varied and far reaching system, both inner-agency and outside expertise were utilized in Objective Two. The in-house task force provided line staff and managers an opportunity to direct their agency's use of available technology. Perhaps most importantly, the task force allowed management to determine how it could best perform the managerial function given the insight and capability of 1990's computer technology.

The outside perspective of a consultant is combined with the in-house task force to maximize their awareness of what's available and how certain applications may adapt to agency needs. The computer expert may not find a unique place in law enforcement agencies. If a position does not exist, the importance of attracting consultants for this purpose is vital.

Objective Three identifies the critical mass and presents an analysis of how to obtain movement into the specific arena perceived necessary. The other techniques outlined on Objective Three are presented in the generic form for consideration of alternatives which could be used to implement the strategic plan.

As a result of this study, two paramount challenges facing police managers today emerged; 1) the need to mesh with progress or be bypassed by the changes it brings; and 2) to direct organizational change or be caught simply reacting to the chaos it may create.

Through the process of preparing this monograph, the writer gained some valuable insight into the future of automation in law enforcement. First of all, it is inevitable. Secondly, those caught unprepared will always be in a reactive position. With the technologies in existence today, all the possibilities outlined in the future scenarios are possible. (Portable lap top computer with direct access to CPU, cellular networks, artificial intelligence, language

identification generation system, voice-activated computers, laser scan of license plates, vehicle disengagement unit, laser fitted handguns, knowledge based systems, expert systems computer aided training, etc.)

And if that's exciting, consider this: recently a futurist predicted that 90% of the technology we will be using in the year 2000 has yet to be invented.

END NOTES

END NOTES

- 1 Sykes, Gary W. "Automation, Management, and the Police Role: The New Performers?" Journal of Police Science and Administration, March 1986, p 24.
- 2 Vandiner, James V. "Coping With the Computer Revolution." Police Chief, The, April 1984, p 42.
- 3 Sykes, Gary W. "Automation, Management, and the Police Role: The New Performers?" Journal of Police Science and Administration, March 1986, p 25.
- 4 Shubin, Lester D. "The Next Twenty Years." Police Chief, The, April 1984, p 33.
- 5 Ibid, p 35.
- 6 Hernandez, Armand P. "Is Law Enforcement Ready for the Artificial Intelligence Explosion?" Police Chief, The, May 1986, p 50.
- 7 Ibid.
- 8 Ibid.
- 9 Zemke, Ron. "Artificial Intelligence: What Trainers Can Learn From The Silicon Frontier." Training, December 1983, p 66.
- 10 Ibid.
- 11 Tafoya, William L. "Artificial Intelligence Research and Development Project of the National Center for the Analysis of Violent Crime at the FBI Academy". Eleventh Annual Law Enforcement Information Systems Symposium, August 1987, p 4-6.
- 12 Ibid, p 11.
- 13 Naisbitt, John. "1984 Megatrends - Ten New Directions Transforming Our Lives". New York: Warner Books, p 9.
- 14 Ibid.
- 15 Ibid.
- 16 _____

- 17 Chafin, Clinton & Gibson, Morris F. "Computer-Assisted Management of Police Reporting Systems." *Police Chief*, The, April 1984, p 4.
- 18 Rosen, Daniel M. "Police and Computers." *Police Magazine*, September 1982, p 10.
- 19 Chafin, Clinton & Gibson, Morris F. "Computer-Assisted Management of Police Reporting Systems." *Police Chief*, The, April 1984, p 33.
- 20 Tafoya, William L. "Into the Future...A Look at the 21st Century". *Law Enforcement Technology*, September-October, 1987, p 20.
- 21 Ibid.
- 22 Ibid.
- 23 Sykes, Gary W. "Automation, Management, and the Police Role: The New Performers?" *Journal of Police Science and Administration*, March 1986, p 29.
- 24 Ibid.
- 25 Ibid.

BIBLIOGRAPHY

BIBLIOGRAPHY

- Beckwith, Burnham, P. "The Next Thousand Years." *Futurist, The*, September-October 1986.
- Black, James K. "Taking a Byte Out of Crime." *Police Chief, The*, 31-34, May 1986.
- Chafin, Clinton & Gibson, Morris F. "Computer-Assisted Management of Police Reporting Systems." *Police Chief, The*, 46-47, April 1984.
- Coady, William. "Automated Link Analysis: Artificial Intelligence-Based Tool for Investigators." *Police Chief, The*, 22-23, September 1985.
- Culley, John A. "On-Site Microcomputers Help Police UN's 40th Anniversary Session." *Police Chief, The*, 38-45, May 1986.
- Dean, William T. & Haynes, Steven E. "Law Enforcement Information Systems." *Police Chief, The*, 44-45, April 1984.
- Egger, Steven. "The New Predators." *Futurist, The*, April 1985.
- Fauley, Franz E. "The New Training Technologies: Their Rocky Road to Acceptance." *Training and Development Journal*, 22-25, December 1983.
- Garr, Doug. "Home is Where the Work Is." *Omni*, December 1984.
- Gladwin, Lee A. "The Impact of Artificial Intelligence on Training." *Training and Development Journal*, 46-47, December 1984.
- Hernandez, Armand P. "Is Law Enforcement Ready for the Artificial Intelligence Explosion?" *Police Chief, The*, 50-52, May 1986.
- Hernandez, Jr., Ernie. "The Social Impact of Computerization In Criminal Justice: Problems With Enforcement, Training, and Keeping Democratic Values." *Journal of California Law Enforcement*, 37-42.

- Hillelsahn, Michael J. "How To Think About CBT." Training and Development Journal, 42-44, December 1984.
- Hoban, Phoebe. "Artificial Intelligence." Omni, December 1983.
- Hunter, Bill. "Not Just More Technology But More Useful Technology." Communications World, 24-29, November 1983.
- Jenkins, Brian Michael. "The Future Course of International Terrorism." Futurist, The, July-August 1987.
- Kull, David. "Matching Workstations to Executives Styles." Computer Designs, October 1984.
- Lab, Steven & Hirschel, J. David. "Predicting Crime From the Weather." Futurist, The, March-April 1987.
- Lammers, Allan H. "Search Group - A Resource For Law Enforcement." Journal of California Law Enforcement, 33-36, 1985.
- Lampert, Anne. "Expert Systems Get Down To Business." Computer Decisions, January 15, 1985.
- Larsen, Erik. "Electronic Sleuths: After Long Hesitancy, Police Departments Use Computers More." Wall Street Journal, The, Monday, November 12, 1984.
- Naisbitt, John. "1984 Megatrends - Ten New Directions Transforming Our Lives". New York: Warner Books.
- Magnus, Margaret & Grossman, Mart. "Computers And The Personnel Department." Personnel Journal, 42-48, April 1985.
- Manson, Donald. "Law Enforcement Information Systems." Police Chief, The, 103-107, March 1984.
- Martin, William F. & Swaton, Norm. "Computer's Aim: Make Police Work Easier, Safer." Western City, 15-16 & 18-19, January 1987.
- Meyer, Gary. "What Every Personnel Manager Should Know About Computers." Personnel Journal, 58-63, August 1984.
- Metts, James R. "The Police Force of Tomorrow." Futurist, The, October 1985.
- Molden, Jack. "Cops and Computers." Law and Order, 12, January 1986.

- Montgomery, Redi and MacDougall, Ellis. "Curing Criminals." Futurist, The, January-February 1986.
- Opper, Susanna. "Keep Corporate Teams On Target." Computer Decisions, November 15, 1984.
- Port, Stephen R. "Issues In Police Automation: An Organizational Anatomy." Journal of California Law Enforcement, 146-154, 1986.
- Probert, John. "Police Telecommunications: The Influence of Computers on Law Enforcement." Police Chief, The, 53-55, May 1986.
- Renfro, William L. "Future Histories." Futurist, The, March-April 1987.
- Reynolds, Angus. "Computer-Based Learning: The Key 'Technological Multiplier' for Technology Transfer." Training and Development Journal, 64-67, October 1982.
- Rosen, Daniel M. "Police and Computers." Police Magazine, 9-13, September 1982.
- Shubin, Lester D. "The Next Twenty Years." Police Chief, The, 33-35, April 1984.
- Stephens, Gene. "Crime & Punishment." Futurist, The, January-February 1987.
- Stephens, Gene & Tafoya, William. "Crime & Justice." Futurist, The, February 1985.
- Sykes, Gary W. "Automation, Management, and the Police Role: The New Performers?" Journal of Police Science and Administration, 24-30, March 1986.
- Tafoya, William L. "Artificial Intelligence Research and Development Project of the National Center for the Analysis of Violent Crime at the FBI Academy". Eleventh Annual Law Enforcement Information Systems Symposium, August 1987.
- _____. "Law Enforcement Beyond the Year 2000." Futurist, The, September-October 1986.
- _____. Into the Future...A Look at the 21st Century". Law Enforcement Technology, September-October, 1987.
- Thomas, Doug. "Law Enforcement Needs to Look Ahead." California Peace Officer, 21-25, March 1987.

- Vandiner, James V. "Coping With the Computer Revolution." Police Chief, The, 42-43, April 1984.
- _____. "New Developments In Computer Systems Aid Police." Law and Order, 49-55, February 1985.
- Wilkenson, Tom. "The Use of Computers in Police Training." Police Chief, The, 48-50, April 1984.
- Williard, Timothy H. "Future Focus." Futurist, The, September-October 1986.
- Wishard, William. "The 21st Century Economy." Futurist, The, May-June 1987.
- Zemke, Ron. "Artificial Intelligence: What Trainers Can Learn From The Silicon Frontier." Training, 65-69, December 1983.
- _____. "Policy Mavens Meet the Microcomputer." Training, 46-48, November 1984.
- "Artificial Intelligence: The Next Big Step In Automation." Office Administration and Automation, October 1984.
- "Computer Navigation Coming To Law Enforcement." Law and Order, 24-26, February 1985.
- "Computer Symposium A Success." Law and Order, 71, November 1985.
- "Financial Incentives Offered to Help Employees Purchase Personal Computers." Management Review, 53, October 1984.
- "The High Cost of the FBI's High-Tech Crime Wars." U.S. News & World Report, November 30, 1987.
- "Local Police Advancing In Use of Computers." Criminal Justice Newsletter, April 1, 1985.
- "Microcomputers: Tools for Local Governments." Management Information Service, Vol. 14, #10, October 1982.
- "Reform '88: Computers Key to Improved Federal Management Systems." Government Executive, October 1984.
- "Science, Technology and the Constitution." U.S. Congress, Office of Technology Assessment, September 1987.

APPENDICES

APPENDIX A

Dr. William L. Tafoya Interview

Background: Dr. William Tafoya is a supervisory special agent with the Federal Bureau of Investigation and is assigned to the Artificial Intelligence Research Project of the National Center for the Analysis of Violent Crime at the FBI Academy in Quantico, Virginia. Dr. Tafoya did his doctoral dissertation on a Delphi Forecast of the Future of Law Enforcement.

Questions and Answers

1 Q Do you know what percent of law enforcement agencies in California have some form of automated crime information system?

A The most recent study that I'm aware of is referred to in an article in the September 1982 issue of Police Magazine titled "Police and Computers - The Revolution That Never Came" by M. Daniel Rosen. This article refers to a 1981 Police Foundation survey of police operational and administrative practices among agencies serving a population of 50,000 or more. One hundred twenty-two (122) agencies responded to the survey and virtually all reported some sort of computer capability. NOTE: In this same article Allan Lammers, a former Deputy Executive Director of Search, estimated that there are about 1,500 state and local law enforcement

agencies - serving a population of 25,000 or more - with some sort of computer service. In this same article Allen Pearson, a former Senior Staff Analyst with IACP, estimated that about ninety percent (90%) of the police agencies with any sort of computer capability are using it for the most ordinary purposes imaginable, basically electronic file cabinets.

2 Q Do you view a paperless society and/or a paperless police department as a viable possibility within the next seven years?

A From now to the year 2,000 I suppose it's possible on a small scale basis (agencies serving a population of 50,000 or less), but not for the bigger agencies. There is a real reluctance among the general public to go completely electronic. The expanded use of computers has actually brought on a paper explosion.

3 Q Do you feel law enforcement can effectively deal with computer crime both today and in the future?

A Right now we're probably at the break even point with "cyber crooks", but what we're doing now may not keep us abreast very long. By 1995 we will probably be overwhelmed and will need specialists to deal with the sophistication involved. There is an article in the November 30, 1987 issue of U.S. News and World Report "Wars". The article points out that when Judge William Webster took over as Director he swelled the FBI budget

in nine years from \$622 million to \$1.3 billion, spending hundreds of millions of dollars for high-tech hardware. Capitol Hill critics, who, citing ballooning costs and unfinished systems, are beginning to ask exactly what kind of return the Bureau is getting from the huge investments. The article cites two major projects that were started within the past decade that are not yet totally operational but are increasing in cost: 1) the Organized Crime Information System (OCIS), and 2) the Digital Voice Privacy (DVP) Network. Bureau officials insist, however, that in an increasingly complex and threatening world, high tech is the way to go.

4 Q Do you foresee a "big brother" issue surfacing to the point that law enforcement's use of computers will be curtailed?

A Yes, definitely. Don Edwards, a California Congressman, an ex-FBI agent and a self-appointed watch dog of FBI technology is helping to keep the "big brother" issue alive and well. Historically people have been afraid that "others" have information about them, a dossier if you will. It is a mind set that will always be with us, people do not want others to know about them and the second half of the quotient is their concern about our inability to protect our information. Today police executives are afraid of

technology anyway, so they begrudgingly have it. If law enforcement doesn't establish impregnable quality control measures in informational systems with updated and accurate information, they will continue to fuel the "big brother" syndrome.

5 Q Do you think the State of California, through legislation, will provide funding or incentives to assist law enforcement agencies who want to automate?

A Yes, but it will be a very slow process. The State of Illinois, through the PIMS system, and Florida are assisting local agencies with their automation endeavors.

6 Q Are you aware of any agency that can assist a law enforcement agency who is considering automation?

A On a small scale, consultants. Also, the Institute of Police Technology and Management.

7 Q Do you foresee a governing body legislating law enforcement's use of computers?

A Don Edwards who chairs the House Subcommittee on Civil and Constitutional Rights doesn't necessarily legislate law enforcement's use of computers, but he does "block" a lot of requests that must pass through his committee.

8 Q Do you foresee police agencies interfacing (exchanging crime analysis types of information) in a statewide network?

A Reasonable cost effective technology is now available to do that, but it probably won't happen because of the fear of sharing information and not wanting to give up control. If we had enlightened management it could happen but we'll probably continue to share only basic records type data.

9 Q Do you feel law enforcement agencies are being monitored by computer hackers?

A I believe that computer hackers today have the capability to access police agencies that are using telephone modems, but I don't think they are.

10 Q What ways do you foresee law enforcement executives using computers to manage, a scenario if you will?

A Police managers through the use of artificial intelligence will be able to give the computer a given set of circumstances on just about any problem imaginable and receive a list of alternatives. This technology could be used for matching personnel to a specific task (i.e. like assigning a certain officer to a particular beat that has a certain problem such as a lot of racial tension). This technology will also be used in a lot of other types of deployment decisions, in computer-based instruction of officers and for equipment and evidence inventory.

APPENDIX B

David J. Roberts Interview

Background: Mr. Roberts is a Deputy Director for Search Group Inc. and works in the research and statistics program. Search Group Inc. is a consortium of government appointed representatives of the state. Their goal is to improve the operation of the justice system through the use of technology. This is accomplished through research and demonstration projects. The Search operation is funded by grants from the National Institute of Justice, Bureau of Justice assistance and Bureau of Justice statistics. Search Group is divided into three basic divisions:

- 1) Law and Policy
- 2) Systems and Technology
- 3) Research and Statistics

Search has recently completed two software programs that will be released as public domain in the early part of 1988. The two programs are a jail management system and a District Attorney (prosecutor) assistance system. Search also plans to develop a law enforcement records management system. All of this software technology will be offered as public domain.

Questions and Answers

1 Q What percent of law enforcement agencies in California have some form of automated crime information system?

A My guess would be approximately 1/3 or 33%.

NOTE: Mr. Roberts suggested I contact Mr. Quint Hegner from the Department of Justice for data on the number of automated California law enforcement agencies. I contacted Mr. Hegner and he gave me the following information about an automation survey administered by the Department of Justice in 1986. The survey was sent to 730 law enforcement type agencies and 282 agencies responded. There are approximately 475 city police departments and county sheriffs departments. The remaining 255 agencies surveyed were state police, campus police (junior and state college level) and a number of California Highway Patrol offices. From the 282 respondents, the following data was gleaned from these two specific questions:

1) Does your agency now use an automated crime information system? 44% YES

2) Does your agency now use a computer to store or process uniform crime reporting data? 48% YES

Fifty (50) of the two hundred eighty-two (282) respondents serve a population of 100,000 or more. Through the survey and follow-up telephone contacts the Department of Justice got a one hundred percent (100%) response from these large agencies. Eighty-one percent (81%) of the large agencies now use an automated crime information system. Eighty-five (85%) of the large

agencies now use a computer to store or process uniform crime reporting data.

2 Q Do you view a paperless society and/or a paperless police department as a viable possibility within the next seven years?

A No. Computers have increased the amount of paper flow agencies must deal with. Computers can ease the transfer of information, but everyone still wants a copy.

3 Q Do you feel law enforcement can effectively deal with computer crime both today and in the future?

A It's a form of white collar crime and law enforcement is not very effective in that arena. Computer crime can be very difficult to investigate because it is so well hidden. We don't really know what the monetary loss is. There are questions about jurisdiction and technical issues that need to be resolved if we intend to improve our effectiveness.

4 Q Do you foresee a "big brother" issue surfacing to the point that law enforcement use of computers will be curtailed?

A Possibly. The validity of identification documents such as drivers licenses may be the catalyst of a challenge. I foresee a big push for a national identification card and the general public's reluctance to embrace this concept.

5 Q Do you think the State of California, through legislation, will provide funding or incentives to assist law enforcement agencies who want to automate?

A I would like to see that happen, but I don't think it will because of the financial burden. Nationally, ten million dollars was funded to assist law enforcement agencies in adapting to the new BCS requirements. California only got \$300,000 from that project and it's being used for research, not for hardware purchases.

6 Q Are you aware of any agency that can assist a law enforcement agency who is considering automation?

A Search is trying to. We are developing a micro computer guide; it's not going to be a consumer report ranking of different systems, but it will provide an outline of what to contemplate when considering automation. Search also presents classes for law enforcement administrators to teach them how to evaluate hardware and software vendors. (Members of Search will work with vendors, agencies, or both to review whether the proposed system will meet a department's needs.)

7 Q Do you foresee a governing body legislating law enforcement's use of computers?

A No. Congress will probably restrict access to some data bases, but I don't see much beyond that. The day may come when law enforcement will have access to

anyone's fingerprints through driver's license files, but it will probably be restricted to a major case like a homicide.

8 Q Do you foresee police agencies interfacing (exchanging crime analysis type of information) in a statewide network?

A Yes. Some networking is now being done through regional task forces that are working on serial homicides, rapes, child molestations, etc. These task forces have demonstrated the advantages of a networking system. As law enforcement begins to collect more and more information and improves the sophistication of the crime analysis functions, the probability of a statewide networking system increases.

9 Q Do you think law enforcement agencies are being monitored by computer hackers?

A I suspect that it does occur occasionally.

10 Q In what ways do you foresee law enforcement executives using computers to manage, a scenario if you will?

A All levels. Financial management, resource development, patrol allocation, simulating disasters and computer-aided instruction. An executive will be able to sit at his computer and get a report on financial expenditures and a comparison of those expenditures to the budget.

APPENDIX C

Ernie Hernandez, Jr. Interview

Background: Ernie Hernandez Jr. received his Ph.D in Sociology from the University of California at Riverside in 1979. He has worked as a Behavioral Science Research Analyst for the Los Angeles County Sheriff's Department. He was a Staff Manager for AT&T Information Systems. He has his own private consulting practice in systems research. He has recently written personnel management programs for Irvine and Newport Beach Police Departments and a records management system for Irwindale Police Department. He teaches data base management systems through National University and California State University, Long Beach. He is currently a consultant for G.E. Consulting Services.

Questions and Answers

1 Q Do you know what percent of law enforcement agencies in California have some form of automated crime information system?

A Nobody really knows. My guess would be that about 25-35% have some form of computerization.

2 Q Do you view a paperless society and/or a paperless police department as a viable possibility within the next seven years.

A Not a chance! I was recently a panelist at the Institute of Police Technology in Management in

Jacksonville, Florida and that subject was one of the topics discussed. Among most speakers the consensus was that law enforcement's use of computers will not rid them of paper; in fact it is increasing their paper flow. Everyone seems to need a paper trail and this is especially true in law enforcement. Because law enforcement has such a strong need for documentation, I doubt that you will ever see a paperless police department.

3 Q Do you feel law enforcement can effectively deal with computer crime, both today and in the future?

A It's going to be difficult. Right now we can anticipate that most computer crimes will involve electronic transfer of funds and things of that nature. But in the future, who knows? There will probably be large conglomerates stealing information from each other and law enforcement will have a difficult time dealing with these types of problems. Also, law enforcement probably won't be equipped to do so. When the laws crystallize to take care of these kinds of problems, we probably won't be ready to deal with that kind of sophistication. We are moving in the right direction. (Dr. Hernandez is not aware of any agency presently teaching computer technology in a police academy.)

4 Q Do you foresee a "big brother" issue surfacing to the point that law enforcement's use of computers will be curtailed?

A In a way I can see that coming down the line, but its a ways away. California is probably the leader in law enforcement's use of high tech, but the number of police departments using computers is still in the minority. However, the more computerization law enforcement experiences, the greater the chance of misuse. As the misuse increases (like picking up the wrong person for a crime) then we'll start hearing a public outcry. I don't see it as an immediate issue, but it certainly will be down the line.

5 Q Do you think the State of California, through legislation, will provide funding incentives to assist law enforcement agencies who want to automate?

A Maybe yes, maybe no. Legislators are usually reluctant to force law enforcement to do things. I don't think there are any constituencies who would make this an issue before the legislators so if there is no one to motivate them I doubt it will happen. Right now no one is really upset about law enforcement being slow to computerize their functions. Perhaps POST will be the impetus to get this initiated.

6 Q Are you aware of any agency that can assist a law enforcement agency who is considering automation?

A Well there are consultants that specialize in the law enforcement field, then there is the Search Group. Then there are professional societies such as the American Society of Criminology and the Academy of Criminal Justice Sciences.

7 Q Do you foresee a governing body legislating law enforcement's use of computers?

A Not in the immediate future, its probably 10-15 years away. The majority of households are still not using computers and you can translate that to mean that the majority of us are not caring how law enforcement is using computers. Since it is not regulated, law enforcement right now has basically a free ride, but in 10-15 years everything law enforcement does will probably be scrutinized and regulated.

8 Q Do you foresee police agencies interfacing (exchanging crime analysis types of information) in a statewide network?

A I would like to see that happen but there are a lot of political realities preventing it. There is an organization in Southern California called the Los

Angeles Regional Criminal Justice Coordinating Committee which has been in existence for a couple of years. One of the things they are trying to do is establish a network, but it breaks down because no one wants to share information. Because of that constant inter-agency rivalry I don't think it's going to happen. In fact, even within an agency everyone is protecting their own turf and is reluctant to share information.

9 Q Do you feel law enforcement agencies are being monitored by computer hackers?

A I don't have any way of knowing that. I would say that they have the capability but I don't think at this time hackers are interested in us.

10 Q In what ways do you foresee law enforcement executives using computers to manage, a scenario if you will?

A One area I think will increasingly come into vogue is productivity management. Law enforcement executives will be able to evaluate manpower hours expended on a certain function to see if it was warranted. They will also be able to determine what the financial cost was and make the same determination. There will be more management of day to day activities and the line officer will have "big brother" looking over their shoulder all the time, i.e. the vehicle locater systems.

APPENDIX D

Allen Louis Pearson Interview

Background: Mr. Allen Pearson possesses a BA degree in Political Science and an MA in Urban Studies. He spent two years at the Center of Urban Studies, University of Akron in Akron, Ohio. He has 10 year's experience with IACP as a Senior Staff Analyst and 5 years at the Institute of Police Technology and Management (IPTM) as a Micro-computer Section Coordinator.

Questions and Answers

1 Q Do you know what percent of law enforcement agencies in California have some form of automated crime information system?

A No, but you should check with Search Group, Inc.

2 Q Do you view a paperless society and/or a paperless police department as a viable possibility within the next seven years?

A I personally don't. There are two basic issues; 1) the technological need for data processing, there are too many managers who are entrenched in the paper issue (educational problem), and 2) the concern of a legal problem - courts must have original documents. I don't think it is impossible, but it will be awhile (10 or more years) before we are paperless.

3 Q Do you feel law enforcement can effectively deal with computer crime both today and in the future?

A Today, no. Most law enforcement agencies don't have trained personnel who can deal with the types of computer crimes that exist now. I figure that between ninety-five percent (95%) and ninety-nine percent (99%) of the agencies do not have the expertise to investigate computer crimes. This will be a slow process - playing catch up.

4 Q Do you foresee a "big brother" issue surfacing to the point that law enforcement's use of computers will be curtailed?

A No, I think that issue first surfaced in the late 60's and early 70's. At that time several federal studies were completed and they went over abuse of information with a fine tooth comb. The result was, it either defused the issue or remedied some of the problems. An issue that may rise again is the concern people will have over different agencies sharing their data bases.

5 Q Do you think the State of California, through legislation, will provide funding or incentives to assist law enforcement agencies who want to automate?

- A On the national scale, there may be some impetus to assist small agencies, but it will be in small amounts. Agencies will probably find other means of financing computers (i.e. state and federal grants).
- 6 Q Are you aware of any agency that can assist a law enforcement agency who is considering automation?
- A Search, Inc. can give a good general idea of what systems are being used across the county and provide a foundation to start, and the National Criminal Justice Reference Service in Washington, D.C. They have all the major project reports from government studies and will provide the same to agencies. They also have some public domain software available. IACP staff have visited a vast majority of law enforcement agencies for a first hand look at systems and have a good data base as well as some public software. IPTM will do consulting especially in micro computers and local area networks over the telephone.
- 7 Q Do you foresee a governing body legislating law enforcement's use of computers?
- A Yes, in some shape, form or fashion the issue will not be what law enforcement should do, but what law enforcement should not do (government by exception).

This will probably occur on both state and national levels (i.e. you're not supposed to use Social Security numbers, but it's being done today).

8 Q Do you foresee police agencies interfacing (exchanging crime analysis types of information) in a statewide network?

A I see them interchanging data on a local and regional basis. There are some major cases investigated on a state wide level where a data base is shared with other agencies.

9 Q Do you feel law enforcement agencies are being monitored by computer hackers?

A Probably, but probably very few and on a limited basis for very short durations. Most that might get into the system won't know what they're getting into.

10 Q What ways do you foresee law enforcement executives using computers to manage, a scenario if you will?

A From the micro computer standpoint, spread sheet budget forecasting, records management, etc. Most managers just store information, seldom do they retrieve it. To use computers, younger executives are more intuned. It will take a long time before we see any significant impact in the police arena.

APPENDIX E

TRENDS

1. increase in computer literacy
2. decreasing cost of computer hardware
3. computerized records/management information systems, crime analysis, CAD, administrative reports and personnel deployment
4. computerized crime increasing (degree really unknown)
5. increased use of computers
6. computerized traffic control
7. computerized evidence analysis and comparisons
8. shorter work week
9. white collar crime increasing
10. expansion of software capabilities
11. compatibility of technologies decreasing
12. invention of personal computer
13. dual careers
14. communication capabilities increasing (satellite and fiber optics)
15. use of MDT's and hand-held portables increasing
16. paperless society
17. transient society
18. acceptance of computer technology on the upswing
19. use of ATM cards vs. \$ on the upswing

20. capability of computer technology increasing
21. media support
22. majority of jobs information-oriented
23. productivity of employees using computers increasing
24. speed of on-line information access improving
25. drug abuse increasing
26. disparity of work ethics
27. organized crime ever present
28. civil liability issues impacting public resources
29. privatization of the public sector
30. environmental settings (biological and psychological needs)
31. public fear of privacy invasion (big brother syndrome)
32. disability issues
33. legal restraints
34. public fear of terrorism
35. POST influence on management training
36. increase in jail/prison population
37. high school dropout rate decreasing
38. increase in use of private police
39. increase in drug related crimes
40. decrease in qualified applicants for law enforcement
41. feminist and minority movement
42. gay rights
43. increase in violent crime
44. increase in property crime

45. use of public funds for aids research increasing
46. use of contract policing increasing
47. use of robotics increasing
48. stress related retirements
49. shrinking revenues for public entities
50. spending limits result of Propositions 4 & 13
51. increased elimination of middle management positions
52. baby boom generation reaches "middle age"
53. use of consultants in law enforcement increasing
54. continued concern over homeless
55. state use of public retirement funds
56. increase use of binding arbitration by public entities
57. court scrutinization of "employee rights" issues
58. increase entrepreneurship found in municipal government
59. demand for increased leisure time by public employees
60. increased urbanization
61. conservative movement in the majority
62. affirmative actions mandated by courts
63. public employers charged with responsibility of employee physical fitness (tied to liability issues)
64. increased civilianization
65. public concern over criminal justice system victimizing victims
66. law enforcement's inundation with information
67. "generation gap" increasing between management and line personnel

68. management's perception of new recruits includes "unreasonable" expectations
69. public fear of criminal activity affecting them personally

TREND SCREENING FORM

APPENDIX F

CANDIDATE TREND	For purposes of top-level strategic planning in, how valuable would it be to have a really good long-range forecast of the trend?				
	PRICELESS	VERY HELPFUL	HELPFUL	NOT VERY HELPFUL	WORTHLESS
1. increase in computer literacy		X			
2. decreasing cost of computer hardware		X			
3. computerized records/management information systems, crime analysis, CAD, administrative reports and personnel deployment		X			
4. computerized crime increasing (degree really unknown)			X		
5. increased use of computers			X		
6. computerized traffic control			X		
7. computerized evidence analysis and comparisons			X		
8. shorter work week				X	
9. white collar crime increasing				X	
10. expansion of software capabilities exponentially increases through artificial intelligence		X			
11. compatibility of technologies decreasing - advancement in brick "dumb" terminals		X			
12. invention of personal computer			X		

Form 4.1

TREND SCREENING FORM

CANDIDATE TREND	For purposes of top-level strategic planning in, how valuable would it be to have a really good long-range forecast of the trend?				
	PRICELESS	VERY HELPFUL	HELPFUL	NOT VERY HELPFUL	WORTHLESS
13. dual careers				X	
14. communication capabilities increasing (satellite and fiber optics)		X			
15. use of MDTs and hand-held portables increasing		X			
16. paperless society		X			
17. transient society				X	
18. acceptance of computer technology on the upswing			X		
19. use of ATM cards vs. \$ on the upswing			X		
20. capability of computer technology increasing		X			
21. media support			X		
22. majority of jobs information-oriented		X			
23. productivity of employees using computers increasing			X		
24. speed of on-line information access improving			X		

Form 4.1

TREND SCREENING FORM

CANDIDATE TREND	For purposes of top-level strategic planning in, how valuable would it be to have a really good long-range forecast of the trend?				
	PRICELESS	VERY HELPFUL	HELPFUL	NOT VERY HELPFUL	WORTHLESS
25. drug abuse increasing				X	
26. disparity of work ethics				X	
27. organized crime ever present				X	
28. civil liability issues impacting public resources		X			
29. privatization of the public sector			X		
30. environmental settings (biological and psychological needs)			X		
31. public fear of privacy invasion (big brother syndrome)		X			
32. disability issues			X		
33. legal restraints			X		
34. public fear of terrorism			X		
35. POST influence on management training		X			
36. increase in jail/prison population				X	

Form 4.1

TREND SCREENING FORM

CANDIDATE TREND	For purposes of top-level strategic planning in, how valuable would it be to have a really good long-range forecast of the trend?				
	PRICELESS	VERY HELPFUL	HELPFUL	NOT VERY HELPFUL	WORTHLESS
37. high school dropout rate decreasing				X	
38. increase in use of private police			X		
39. increase in drug related crimes				X	
40. decrease in qualified applicants for law enforcement			X		
41. feminist and minority movement				X	
42. gay rights				X	
43. increase in violent crime				X	
44. increase in property crime				X	
45. use of public funds for aids research increasing				X	
46. use of contract policing increasing				X	
47. use of robotics increasing			X		
48. stress related retirements				X	

Form 4.1

TREND SCREENING FORM

CANDIDATE TREND	For purposes of top-level strategic planning in, how valuable would it be to have a really good long-range forecast of the trend?				
	PRICELESS	VERY HELPFUL	HELPFUL	NOT VERY HELPFUL	WORTHLESS
49. shrinking revenues for public entities			X		
50. spending limits result of Propositions 4 and 13			X		
51. increased elimination of middle management positions			X		
52. baby boom generation reaches "middle age"				X	
53. use of consultants in law enforcement increasing			X		
54. continued concern over homeless				X	
55. state use of public retirement funds				X	
56. increase use of binding arbitration by public entities				X	
57. court scrutinization of "employee rights" issues			X		
58. increase entrepreneurship found in municipal government			X		
59. demand for increased leisure time by public employees				X	
60. increased urbanization				X	

Form 4.1

TREND SCREENING FORM

CANDIDATE TREND	For purposes of top-level strategic planning in, how valuable would it be to have a really good long-range forecast of the trend?				
	PRICELESS	VERY HELPFUL	HELPFUL	NOT VERY HELPFUL	WORTHLESS
61. conservative movement in the majority				X	
62. affirmative actions mandated by courts			X		
63. public employers charged with responsibility of employee physical fitness (tied to liability issues)				X	
64. increased civilianization			X		
65. public concern over criminal justice system victimizing victims				X	
66. law enforcement's inundation with information		X			
67. "generation gap" increasing between management and line personnel				X	
68. management's perception of new recruits includes "unreasonable" expectations				X	
69. public fear of criminal activity affecting them personally				X	

Form 4.1

APPENDIX G

TREND EVALUATION CHART

TREND STATEMENT	LEVEL OF THE TREND (RATIO: TODAY=100)			
	5 YEARS AGO	TODAY	"WILL BE" IN 7 YEARS	"SHOULD BE" IN 7 YEARS
1. COMPUTERIZED LAW ENFORCEMENT FUNCTIONS	50	100	H 600 L 400 A 500	H 800 L 600 A 700
2. HARDWARE TECHNOLOGY ADVANCEMENT-BRICK "DUMB" TERMINALS	0	100	H 700 L 500 A 600	H 800 L 600 A 700
3. SOFTWARE TECHNOLOGY- EXPONENTIAL ADVANCEMENTS THROUGH ARTIFICIAL INTELLIGENCE	20	100	H 900 L 700 A 800	H 1,200 L 950 A 1,000
4. INFORMATION INUNDATION IN LAW ENFORCEMENT	40	100	H 650 L 250 A 500	H 800 L 600 A 700
5. BIG BROTHER SYNDROME (PRIVACY INVASION)	30	100	H 300 L 100 A 200	H 250 L 50 A 100

APPENDIX H

EVENTS

1. Governor signs legislation which makes funds available for computerization of all California law enforcement agencies.
2. A new technology is developed that enables all major computer systems to be compatible and subsequently enhances a state-wide networking system.
3. Organized crime member arrested for accessing a large metropolitan crime analysis file to enhance his narcotics activities.
4. High school drop out rate increases to 40%.
5. State adopts growth limitations on California cities with populations of 100,000 plus.
6. Low unemployment rate in California (less than 3%) severely impacts recruitment of qualified police officers.
7. A special interest group targets law enforcement automation processes and generates a major negative publicity campaign.
8. California Supreme Court mandates that all public entities adopt and initiate comparable worth policies.
9. Ten percent (10%) of California police chiefs and sheriffs are women.

10. Computer hacker arrested for accessing and pirating various data base files from a police agency.
11. State and local discounts to California law enforcement agencies for computer equipment (hardware and software) are discontinued.
12. Federal court severely restricts funds used by POST to subsidize training of California law enforcement officers.
13. California Supreme Court upholds constitutionality of city ordinance which limits law enforcement's use of information in data base files
14. California's Public Employees Retirement System (PERS) files for Chapter 11 under bankruptcy procedures.
15. California Appellate Court upholds constitutionality of police union strikes.
16. Terrorist group successfully sabotages computer system of large metropolitan police agency.
17. Computer hacker exposed and arrested for capturing a policy agency's computerized files by using an electro magnetic radiation device.
18. Federal Court rules that law enforcement must provide hard copies of all data contained in automated files.
19. Computer technology developed that enables portable computers with voice synthesizers to interpret foreign languages.

20. Computer technology developed that enables police officers to receive both verbal and printed commands from dispatch center.
21. Computer technology perfected that allows verbal entry into computer systems.
22. Computer technology developed that allows "dumb" terminals to link with other computer systems through the use of satellites, fiber optics or radio waves.
23. Proposition 4 (spending limitations) challenged on constitutional merits but upheld by U.S. Supreme Court.
24. A devastating earthquake occurs in California, causing extensive property destruction and severely restricts power sources for six months or longer.
25. State mandates that all patrol cars be equipped with MDTs.
26. Major riots by minority groups occur in several large California cities.
27. State mandates that all BCS reports will be computerized.
28. State mandates computer tracking of all prison inmates released on parole.
29. Aids reaches epidemic proportions, killing 10,000 Californians in a 3 month period.
30. POST mandates that all California police academies provide a minimum of 100 hours of computer training including hands on experience.

31. National government initiates severe trade restrictions on computer parts from foreign countries.

APPENDIX I

STAKEHOLDERS

1. Sworn Personnel
2. Non-Sworn Personnel
3. Sworn Management
4. Non-Sworn Management
5. Taxpayers
6. Media
7. Organized Crime
8. Police Associations (unions)
9. Organized Labor Unionrs (i.e. ACLU)
10. Software Vendors
11. Hardware Vendors
12. Minority Groups
13. Women in Work Force
14. Seniors
15. Local Politicians (City Council/Board of Supervisors)
16. State and Federal Politicians
17. Administrative Staff (City Manager/County Administrator)
18. City Department Heads
19. Judges/Courts
20. Office of Criminal Justice Planning (State Funding Agency)
21. Office of Traffic Safety (State Funding Agency)
22. California Peace Officer's Association (CPOA)

23. California Police Chief's Association (CPCA)
24. California State Sheriff's Association (CSSA)
25. Peace Officers Research Association of California (PORAC)
26. Women Peace Officer's Association (WPOA)
27. Commission on Peace Officer Standards and Training (POST)
28. Insurance Companies
29. Groups Concerned with Civil Liabilities
30. Private Security Companies
31. Electronic Industry
32. Attorneys
33. International Association of Chiefs of Police (IACP)
34. Search Group, Inc.
35. Technology Researchers
36. Consumer Groups