HOW WILL THE USE OF THE INTERNET IN A MOBILE COMPUTING ENVIRONMENT CHANGE THE PATROL FUNCTION IN LAW ENFORCEMENT AGENCIES BY 2007?

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

by

Mark Yokoyama, Captain
Newark Police Department

Command College XXXIII

Sacramento, California

November 2002

33-0668

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

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

Managing the future means influencing the future: creating it, constraining it, and adapting to it. A FUTURES study points the way.

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

Copyright 2002
California Commission on Peace Officer Standards and Training

ACKNOWLEDGEMENTS

I wish to express my sincere thanks to the many individuals and teams that were involved with this project. Chief John Robertson, who has been a personal mentor of mine for many years, has placed his faith in me by encouraging me to explore technological developments for use within the organization and industry. Matt Breen, Ron LaSalle, Misa Leal and other industry experts provided me with the technical guidance necessary to make this project possible. Chief Tom Soberanes, POST Consultant Alicia Powers, and Consultant Tom Esensten have made the entire Command College process a learning environment that has positively impacted my way of thinking and planning for the future of law enforcement. Finally, I would like to send a special thanks to my family, who provided the moral support necessary to complete this project.

TABLE OF CONTENTS

	Page
Chapter One	
INTERNET AND TELECOMMUNICATIONS TECHNOLOGY	1
Introduction	1
Historical Development	2
Wireless Communications and Law Enforcement	5
Chapter Two	
FUTURES STUDY OF MOBILE COMPUTING AND THE INTERNET	8
Forecasting of Trends and Events	8
Nominal Group Technique	9
Summary Trend Table and Analysis	10
Trends	12
Summary Event Table and Analysis	16
Events	17
Cross Impact Analysis	21
Scenarios	23
Pessimistic Scenario	24
Optimistic Scenario	26
Normative Scenario	28
Chapter Three	
STRATEGIC PLAN	31
Strategic Planning	31

Situation Analysis 32

Stakeholder and Snail Darter Analysis 36

Strategies 39

Chapter Four

TRANSITION MANAGEMENT 41

Transition Management and Commitment Planning 41

Critical Mass 42

Responsibility Charting 43

Implementation 44

Chapter Five

FINDINGS AND CONCLUSIONS 47

THE APPENDICES

Appendix A - List of Trends 52

Appendix B - List of Events 53

ENDNOTES 55

BIBLIOGRAPHY 57

CHAPTER ONE

INTERNET AND TELECOMMUNICATIONS TECHNOLOGY

Introduction

In recent years, law enforcement agencies across California and the United States have increasingly utilized technologies associated with computers. It would not be uncommon in today's environment to find a police officer with a laptop or mobile computer in his or her patrol vehicle writing a police report and transmitting that same report from the field directly to their police station for supervisory approval. It would also not be uncommon to find police officers querying various databases from their police cars using mobile computers or cellular phones to conduct investigations. Research by the U.S. Department of Justice, Bureau of Justice Statistics discovered that of the 85 municipal law enforcement agencies employing more than 100 sworn officers in California, 59 had mobile computers/terminals in their patrol vehicles in the year 2001.

As society becomes more dependent upon Internet applications, we can assume that law enforcement will also follow this path. The web site Officer.com has 462 links to California law enforcement agency web sites in California. Of those, 281 are municipal law enforcement agencies, including sheriff's departments. There are 394 municipal agencies in California.[1] Although web sites may be used in different ways by various agencies, what these statistics indicate is that a large percentage of law enforcement agencies are utilizing the Internet already.

With the advent of technologies that allow access to the Internet using wireless connectivity, law enforcement must consider its future implications. Private industry is utilizing Internet applications via mobile computers to maintain communications with

customers and company representatives and to conduct daily business operations just as if they were at a traditional desk in a business office. Law enforcement agencies have historically followed the lead of private industry in regards to business applications. As can be seen from statistics previously mentioned, the Internet is already being utilized by law enforcement and thus the obvious question is, "How and when will the Internet be used by law enforcement in a mobile computing environment?" Ignoring such a question could negatively affect public safety and efficient policing strategies.

Historical Developments of the Internet and Telecommunications

The use of the Internet and cellular phone technology has, on its own, changed the way human beings live their daily lives. The Internet has grown from its original intent of network computers at research institutions across the United States in the 1960s to a powerful communications medium. Applications of the Internet are continually evolving, creating new uses for business, government, and individuals, thus impacting cultures and age groups all over the world. This cultural and generation shift is not limited to North America or wealthy nations, but has spread to developing and Third World countries as well.[2] Consider the following statistics from just the United States: Over half of the country's 105 million households have computers; 42 percent could log on to the web in 2000 and nearly 90 percent of all school-aged children age 6 to 17 had access to computers either at home or at school. Nearly two-thirds of all children between the ages of 3 and 17 lived in homes with computers and nearly one-third of children in that age range have gone online.[3] When combined with the number of cellular phone users worldwide, estimated at approximately 1 billion users, communication capabilities are endless.

The automotive industry has made great strides in taking advantage of the plethora of communication capabilities through a technology that has been coined "telematics." Although still a term defining itself, Telematics is a mobile communications service delivered wirelessly to in-vehicle devices. Traditional telematic services have been used to provide navigation services, track stolen cars, performing roadside diagnostics of vehicle operations, provide remote door unlock services, calling emergency road-side assistance, automatically notifying authorities of vehicles in distress, and most recently, provide concierge services. The most commonly known service is a product used by General Motor's called "OnStar." The OnStar product has been in operation and continued development since 1996. To date, OnStar has almost 2 million subscribers and, on average, provides the following on a monthly basis: 200,000 routing calls, 15,000 door unlocks, 14,000 roadside dispatches, 300 air-bag deployments and 375 stolen vehicles located.[4] OnStar most recently introduced a hands free, voice activated cellular phone service, as well as a voice activated, hands free Internet platform that will read email, news, weather, traffic reports, stock quotes, sports scores, and so forth to work in conjunction with its other telematic services.

The Ford Motor Company, with its stronghold on providing law enforcement vehicles to the industry, has entered into the telematics arena as well through a joint venture with Qualcomm Inc., called "Wingcast." This joint venture has created a vision to develop and deliver wireless mobility and information services that will bring voice, entertainment, Internet access, and safety services into cars and trucks similar to GM's OnStar. One key differentiator between Wingcast and other telematic service providers is the accessibility to all applications and services wherever they may be. The car will

become a so-called mobile computer to the Wingcast server and Wingcast services, and applications will be available both from within the vehicle and outside of the vehicle using devices such as hand-held personal digital assistants, cellular phones, and other hand-held computer devices. Information will flow effortlessly from one device to another, regardless of whether the user is at home, in the car, or in the office. The vehicle is a modified mobile docking station for more advanced information and entertainment services while still performing basic communication, notification, and security services.[5]

What is particularly interesting about this technology is its evolutionary path. What started out as a security feature to allow for the tracking of stolen vehicles has now transformed into a device that allows for live communication, similar to dispatch services and voice controlled Internet services. In some vehicles, small dash mounted monitors are installed to allow for global positioning satellite (GPS) functionality that provides mapping services. The evolution continues as companies such as Microsoft, Motorola, IBM, Palm, and telecom carriers such as Sprint and Verizon enter the industry, all vying for position to establish a foothold in the telematic industry.

The next generation internet, termed 3G, or third generation and beyond, brings with it a new phenomenon when combined with telematics. As can be seen from the evolutionary path of telematics, the framework for the same communication capabilities and more one receives from their home or desktop computer will be available from a mobile environment. The term 3G is shorthand for third generation, and it refers to a technical specification for wireless data and communications to travel at much faster rates than what has been possible in the past. The first and second generation Internet were analog and digital networks, while 3G has migrated to a new digital form called packet-

switched networks. In very simple terms, the speed of 3G technology will allow for traditional e-mail and text based services, as well as multimedia data such as video mail, video news clips, video conferencing, television, music, and photos to move within a wireless, mobile environment and at a faster pace. The 3G terminals would have more varieties than those of 2G, mostly in the form of mobile phones, but with larger screens for displaying Internet pages or the face of the person being talked to. There will be smaller smart phones with web browsing and e-mail capabilities. Moreover, videophones, wrist communicators, palmtop computers, and radio modem cards for portable computers will also be available.[6]

Considering the following facts, one can easily see the trend of mobile communications. The average driver spends more than two hours a day in his or her car; some 70% of all mobile calls originate in a car. By the year 2005, 84% of new cars sold will have telematics available as either standard or optional equipment.[7] By 2002 more than 1 billion people will own a cellular phone; by the end of 2002, the number of mobile Internet users will exceed traditional PC connections.[8]

Wireless Communications and Law Enforcement

From a law enforcement perspective, one can see many positive and negative scenarios occurring with regards to the use of mobile services. Just on its surface, critics will focus upon the inherent safety issues that revolve around operating any device in a mobile environment. One must only look at the current media reports and traffic statistics regarding vehicular accidents related to mobile phone use as a result of its related distractions. From a police management perspective, critics will argue the

maintenance cost for upkeep of such a system or a potential abuse of the system regarding access to the Internet. Information Services (IS) personnel may argue integration and security issues involved with interoperability between the Internet, Intranet, and national, state, and local databases.

From a positive standpoint, mobile services will allow police officers to have access to a true office in a mobile environment and have interoperability of services that were not available in the past. The following are some services or scenarios that will keep police officers in the field and provide them with access to more information to carry out their job functions:

- Video conferencing for roll calls, court appearances, or meetings from a field environment; instant access to community members using phone and video lines
- POST Training via Internet access and on-line education
- Live video surveillance or remote situation analysis from a distant location
- Pictures of missing children or a wanted suspect
- Instant fingerprint or facial recognition analysis
- E-mail capabilities to community members from the field
- Instant communication or interoperability with allied agencies from the field
- Access to building plans and other mapping functions for tactical situations
- Access to web based legal and investigative resources

The number of Internet users worldwide will nearly triple, from 130 million in 1999 to 362 million in 2003. The U.S. share of the global Internet-user population in that time will shrink from about 42% to 36%.[9] This trend does not necessarily tell us, that Internet

use will decrease in the U.S., rather it is telling us, that Internet use will increase worldwide.

Criminals, terrorists, and computer hackers are taking advantage of these technologies to carry out their missions and criminal enterprises because of their accessibility to technology and communications. On the other hand, the lack of law enforcement communications interoperability across the state and nation creates a large void when it comes to communications and information sharing among law enforcement professionals. Today, emergency incidents increasingly require a high level of multi-agency and multi-functional response by law enforcement personnel. The same can be said for pre-incident planning and intelligence sharing.

Law enforcement must be proactive in finding new ways to utilize the same technology that is being used against them and law-abiding citizens. As a result, it is incumbent upon police managers, industry experts, and Information Technology Analysts to work in partnership to take advantage of this resource.

The following chapter will provide information about a probable future by forecasting trends and events as it relates to Internet and telecommunications technology.

CHAPTER TWO

FUTURES STUDY OF MOBILE COMPUTING AND THE INTERNET

Forecasting of Trends and Events

The word future is defined in the American Heritage dictionary as, "The indefinite period of time yet to be." The assumption here is that there will always be a future and thus society will need to continually adjust throughout lifetime to function within society. Organizations will also need to make these same types of adjustments or risk a decline in organizational efficiency and effectiveness.

The difference between a good organization and those organizations that are leaders of the industry, is the ability and follow through of the latter in forecasting applicable future trends and events as it applies to their industry. Utilizing such conceptual skills in forecasting the future allows organizations to plan and make informed decisions that directly affect goals, values, and direction. By anticipating what the future holds, one can intellectually prepare for the future, as opposed to changing with no planning once the future has arrived. Abraham Lincoln said, "If we could first know where we are, and whither we are tending, we could better judge what to do, and how to do it."[10]

Considering the learning point by Abraham Lincoln and relating it to the technological revolution, it should be of particular interest to leaders to consider future applications of technology. The technological revolution has introduced various pieces of equipment, software, computers, and so forth to assist law enforcement in its mission. Based upon the history and current application of the Internet, the increased use of laptop

computers, and the expansion of wireless communications in the law enforcement field, one can assume that some nexus occurs in all three of these areas. This project considers the technological integration of mobile computers and the Internet for police officers in the field.

To better explore this issue and forecast the future, research is necessary to form proper conclusions and strategic planning methods. A Nominal Group Technique (NGT) process was conducted to make this possible. The NGT is a structured process that utilizes a diverse group of people with different experiences and backgrounds to solicit opinions and thoughts regarding a particular issue. Trends and events are identified and ultimately ranked to provide focus for the issue in question. In this case, the issue is the use of the Internet in a mobile computing environment by the patrol function within law enforcement organizations.

Trends are a series of occurrences over time that indicate a particular direction of an issue. Events, on the other hand, are singular occurrences that can positively or negatively impact the issue. When considered together, both have the ability to assist in futures forecasting with careful analyses and cross-analyses.

Nominal Group Technique

The NGT consisted of nine individuals with diverse experiences and backgrounds to allow for creative input and discussion. Their backgrounds included: a police manager, police officer and police dispatcher; a municipal information systems manager; a full-time college student; a retired produce manager; a full-time stay-at-home mom; a computer sales representative; and a wireless communications system engineer.

The NGT panel was thoroughly briefed ahead of time with information about futures forecasting, specific technologies related to the issue, and details about the NGT process. This was also repeated on the day of the NGT. A personal assistant recorded information collected during the NGT.

During the course of this exercise, the panelists looked at two different dimensions, trends and events, and their potential applications of this technology (Appendix A and B). After the panelists collectively identified those trends and events and pared them down to what they determined to be the top five, a mathematical calculation as described below, was used to quantify their ideas and opinions. The results of those calculations identified disparities within the group on each of the trends and events that were evaluated. This process generated thoughtful and interesting discussions as various members of the group attempted to persuade others to think differently about their particular assessments. The following pages summarize the results of the NGT.

Summary Trend Table and Analysis

After the panelists were asked to rank their top five trends for this issue, they were instructed to provide an estimated numerical value indicating the level of the trend five years in the past, five years into the future, and 10 years into the future. As a baseline and point of reference, the numerical value of 100 was presumed as a value for the present year. The applicants were also asked to place a value, relative to the level of concern about the trend relative to the issue, using a scale of 1 to10, with 10 being the highest level of concern. At the conclusion, the values were averaged (rounded to the nearest tenth) and produced the following results:

TRENDS	-5 Years	Today	+5 Years	+10 Years	Concern (1-10)
T1: Level of Homeland Security	5	100	250	375	7
T2: Use of "Instant messaging" and video conferencing	30	100	450	725	6
T3: Use of telematics technology	5	100	600	900	8
T4: Capacity of bandwidth technology	25	100	375	750	9
T5: Amount of Internet terrorism acts	20	100	500	850	10

In looking at the trend table, one can see that the level of the trends was much lower in the eyes of the panelists five years in the past. This was attributed to the fact that technology and its related components were still in their development stage and finding their place in society. The learning curve of the general public was not advancing as quickly as technological advancements. Five years ago, society was still educating themselves and exploring the use and applications of computers. During this same time period, the technology industry was developing newer products that will be faster, smaller, and smarter with greater applications for the user. The unfortunate terrorist attacks of September 11, 2002 contributed significantly to the panel's belief that homeland security was virtually non-existent with only minimal levels of concern five years ago.

On the other hand, five and ten years into the future, the panelists saw the same trends significantly increase. The change was attributed to the group's belief that society would adapt to the technology and that technology would continue to evolve and bifurcate into a new set of trends. All of the trends were believed to have a strong impact on the issue of mobile Internet use by the patrol function. The following is an analysis of each trend:

Trend 1: Level of Homeland Security

Five years ago, plans and resources dedicated to homeland security were of little concern to American society. However, as a result of the terrorist attacks on September 11, 2001 against the United States, the panelists felt that security infrastructures would significantly increase. Part of this infrastructure includes improving communications between local, state, and federal law enforcement agencies. These communication improvements will rely upon systems like the Internet that can relay information quickly through such technology as satellite and cellular systems.

Due to the heightened awareness and current events surrounding homeland security, funding is expected to increase or be diverted to law enforcement at all levels, especially at the federal level through the Office of Homeland Security. Over the course of the next five years, the panel felt that systems, procedures, and processes would be improved, but will only slightly increase and level off after 2007 as society regains its sense of security.

Trend 2: Use of Instant Messaging technology that incorporates video conferencing

The use of instant messaging technology has significantly increased over the past several years and it is anticipated to increase well into the future. Video conferencing has seen a new interest after the terrorist events of September 11th that has brought video conferencing to a new front, as people are less inclined to fly. With instant messaging, officers in the field can communicate directly with community members and allied law enforcement agencies in real time. Video conferencing brings with it a new list of applications to law enforcement such as: court appearances from the field, video conferencing with community members or department members, or even training courses produced live from out-of-area locations. More and more households are accessing friends and relatives with instant messaging and video technology, and even doing so via their traditional television sets (i.e., AOL TV and Web TV). The panel believed that this trend had great potential for growth into law enforcement applications.

Trend 3: Use of telematics technology

By the end of 2002, more than 1 million Ford cars will be equipped with Internet capabilities allowing car occupants to access the Internet through an in-car computer and dash mounted monitor.[11] This technology called telematics combines electronics with that of telecommunications. Telematics moves well beyond current products that offer mapping and roadside assistance and will create a true mobile office system. Ford and Qualcomm, in a joint venture, have developed Wingcast, with a vision "to turn the automobile into a prominent mobile Internet portal."[12] With Ford's control of police vehicles, the availability of Internet access becoming a standard feature in police vehicles may become a reality, just as a CD player is now. With the Next Generation Internet on

the horizon, fingerprints, photos, live GPS mapping, video conferencing, court arraignments, training, e-mail, calls for service, direct links to the community and immediate links to law enforcement agencies all over the world will create a true office within a moving vehicle for field officers.

The panelists saw this trend in technology to have both positive and negative consequences for law enforcement, especially if the general public had standard access to the Internet via their automobiles. The panel felt that there would be increased demands for service placed on law enforcement due to the increased availability of a communication medium. Although the demands may be legitimate, the impact would be similar to the introductory years of the cellular phone when law enforcement calls for service increased due to ease of instant communication. However, telematics as a communication tool for law enforcement was seen as having great potential with significant growth within the next 10 years. The panel placed a stronger level of concern on this area for fear that the learning curve and adaptability of such technology will meet resistance by traditional officers and leaders in the profession. Any resistance could in fact limit the potential success of such an endeavor.

Trend 4: Capacity of bandwidth technology

In order for law enforcement to take full advantage of the Internet in a wireless mobile environment, bandwidth must expand to be able to transfer such things as photos and videos in a timely manner. Expanding bandwidth was described as moving from analog phone lines to that of cable, DSL (digital), T1 phones lines, fiber optics, satellite systems, and General Packet Radio System (GPRS) wireless technology, an expanded radio technology.

Five years ago, this technology was in its infancy and could not be adequately supplied to front line law enforcement officers. However, with the increased demand from businesses and private citizens desiring the ability to send such things as videos to friends, family, and colleagues, bandwidth technology is predicted to greatly expand over the next 5 to 10 years, thus allowing law enforcement to enter into this field. Should the demand for this technology decrease, it would significantly impact law enforcement applications, as the expansion of bandwidth by the telecommunication industry may slow in its research and production. Should this area continue to grow, it is expected to significantly impact the issue in question. The level of concern for this area was particularly high due to the fact that its application to law enforcement services was deemed critical. Should there be any slow down of technology development, abandonment of the technology or become cost prohibitive, services to the community could diminish instead of flourish.

Trend 5: Amount of Internet terrorism acts

Acts of terrorism will continue to increase well into the future and these so-called acts will utilize the Internet as a tool. Targets will be financial institutions, governmental agencies, and other critical infrastructures. The panelists discussed the possibility of local law enforcement using the Internet as a tool to fight terrorism. Should this become a reality, the Internet could become a law enforcement tool that is as common as a police radio or the telephone. The Internet will not only help fight terrorism, but will also allow law enforcement agencies to share information. Panelists criticized information-sharing as a poor or non-existent practice in the past, but it is a critical component of our future homeland security efforts.

The panelists found this area to have the highest level of concern on law enforcement applications of the Internet from a mobile patrol environment. It was felt that should security measures and regulatory measures against the Internet not be improved or implemented, law enforcement infrastructures could be vulnerable.

Summary Event Table and Analysis

Events, for the purposes of the NGT, are described as singular occurrences that can positively or negatively impact an issue. After the panelists were asked to rank their top five events for this issue, they were instructed to establish the probability of each events occurrence. The summary event table below identifies in its first column the event title, followed by the first year probability of occurrence exceeds zero, the probability that the event will occur within 5 years (100 = certainty), the probability that event will occur within 10 years (100 = certainty) and the positive or negative impact that event would have on the issue. At the conclusion, the values were averaged (rounded to the nearest tenth) and produced the following results:

EVENT	YEAR >0	+5	+10	IMPACT -10 to +10
E1: Computer aided and Internet driven technology replace telephones, televisions, VCR's, and appliances	4	75	90	-9
E2: First police agency implements Technology Based Policing	3	50	85	+7
E3: Legislation enacted regulating use of the Internet	3	85	100	+10
E4: Cyber terrorists hack into law enforcement and databases, critically altering and/or deleting data	2	50	75	-10
E5: Video and other camera technology results in the first capture of criminals and terrorists	3	50	90	+7

Event 1: Telephones, televisions, VCR's, appliances and other electronic equipment are replaced by Internet controlled computer-aided systems.

New computer aided technology will replace the standard light switch, remote controls, telephones and television sets in homes. These electronic devices will be controlled through a computer workstation that accesses the Internet allowing homeowners to control devices from remote locations. Although millions of people across the United States have access to computers and have utilized the Internet in some means, there is another part of society that has not used the services of the Internet. The so-called senior population, which has been said to be the fastest growing population in the United States,[13] grew up during a generation that had no dependency on computers. As a result, this population has secluded itself from certain technologies that exist today, like the Internet.

Should law enforcement agencies, or society in general, move toward a greater reliance on Internet based communications, it may find itself segregating itself from its largest population group. As a result, a shift towards technologies such as networked neighborhoods, video conferencing, e-mail/instant messaging, Technology Based Policing, and other governmental services may be slowed due to this generation gap. Society may find itself utilizing several forms of communication to satisfy both the Baby Boomers, Generation "Y" and "X" populations, and beyond.

The panel felt this event would have a significant negative impact on the use of the Internet by law enforcement patrol officers. The rationale behind such negative impact was based upon the assumption that its various applications would be limited to segments of the population, as opposed to the population at large.

Event 2: First police agency implements Technology Based Policing

Community Policing will move into a new generation that requires interaction with the community using e-mail, instant messaging, video and other interactive technology. This model of policing will be coined "Community and Technology Based Policing." With the large percentage of households that maintain computers and Internet access, including those that maintain mobile communication devices, this will push law enforcement to shift its emphasis to this technology. Just as all law enforcement agencies are being pushed to upgrade their 911 phone systems to accommodate the cellular industry, they will need to do the same for the Internet and other wireless technology industries. It was felt that proactive agencies will begin using this to supplement Community Policing in as early as three years, with a large jump within the industry in 10 years.

Event 3: Legislation enacted regulating use of the Internet.

After much discussion, the panel felt that legislative acts regulating access and use of the Internet will greatly impact law enforcement's future use of the technology. Just as the use of the telephone and radio technology is regulated by such entities as the Federal Communications Commission and the Public Utilities Commission, the panel projected that the Internet would soon fall under such purview within the United States. When such regulation does occur, controls will be set regarding fair pricing for access to the Internet, thereby creating a system for access by all classes (wealthy and poor). Standards will also be set for universal broadband access enabling "always on" high speed connections enabling the use of such things as video to be sent and received via the Internet. Should this occur, law enforcement will find itself with another mode of

communication to community members, and vice versa, similar to the mass availability of telephone communications.

The panel saw this event as having a significant impact on the issue due to its overlapping financial and productivity outcomes. The impact was seen as positive due to the increased functionality of the technology for law enforcement applications. However, it was also discussed that such an event producing wide accessibility to the Internet created by legislation would create an unmanageable influx of communications to police agencies and increased victimization of Internet users.

Event 4: Cyber terrorists will hack into law enforcement databases, critically altering and/or deleting data.

The panel felt that there was a possibility that cyber terrorists will access or hack into law enforcement data files creating a denial of service for law enforcement entities, committing other acts such as changing criminal history information and/or deleting files, or permanently corrupting the system, and so forth. With the evolving expertise of individuals in the computer field and the continued demand well into the future for this expertise, it is expected that this type of activity will be the crime of the future. The panel had a lengthy discussion as to selecting a rate of probability of this to occur, as some felt that the knowledge and skill already exists. It was also felt that some form of this event has probably already occurred. Other panelists felt that security features were sufficiently in place to prevent or mitigate the degree of such an attack. Although the impact of this event would be very negative to the use of the Internet in a mobile environment by law enforcement in the field, a compromise was reached by the panelists

with regards to the probability of this event occurring. The overall consensus was that the event could possibly occur in as early as two years, but was not highly probable.

Event 5: The use of video and other camera technology results in the first capture of a criminal.

Video technology will allow officers in the field to receive streaming video directly into the patrol vehicle with good clarity. Such video would be received from cameras strategically placed throughout a geographical area panning for illegal activity and/or scanning crowds utilizing facial scanning technology. The associated software will compare faces caught on video with that of known or wanted criminals and terrorists, thereby alerting officers to potential threats. Such technology would also be linked to alarm systems that, when activated, would show live video to officers in the field of the location where the alarm was activated from (i.e. banks and liquor stores). The panel felt that this technology was readily available at this time, but felt given the terrorist acts against the United States on September 11, 2001, this technology would be refined in the next few years and would be widely available and in use within five years. The impact to law enforcement goals and missions would be highly positive.

Cross Impact Analysis

Upon completion of the panel's discussion ranking and analyzing of the trends and events, the panel was asked to conduct a Cross Impact Analysis comparing each event with each trend. The question posed to the panel was, "If the listed event were to occur, what impact would this event have on the listed trend?" The impact was based on a numerical value of –5 having the most negative impact to +5 having the most positive

impact. A zero rating indicated no measurable influence or impact. This analysis allowed for a critical review and discussion of various overlapping values, impacts, and concerns, so as to allow for the preparation of various scenarios related to the issue. The Cross Impact Analysis provided for a much more informed or educated strategic planning process.

Cross Impact Analysis Table

Scale: +5 to 0 - 5 to 0	T1 Homeland Security	T2 Instant Messaging / Video Conferencing	T3 "Telematics" Technology	T4 Increased Bandwidth Technology	T5 Amount of Internet Terrorism
E1: Generation Gaps	-4	-3	+2	0	0
E2: Technology Based Policing	+1	+3	+2	+3	+1
E3: Legislation of Internet	+3	+2	0	+4	-1
E4: Cyber Terrorism	-4	-5	-1	-3	+5
E5: Video Technology	+4	+5	+1	+2	0

Based upon comments, conversations, and the analyses from the panelists, it appears that Internet technology and its related functions will have a great impact on law enforcement services ranging from Community & Technology Based Policing to criminal apprehension. The panelists felt the largest challenge to the success of this endeavor will be reducing the potential of terrorist events from computer hacking to assaults on other communication infrastructures. There is no doubt that there are many benefits to this technology, but what it will come down to is how much law enforcement and

governmental agencies are willing to risk and fight for introducing this technology to its full capacity. It is not whether this technology will be available, or how useful it will be, as this is apparent based on the panelists' assessments, but rather how well the industry and profession create a secure wireless communication transaction and educate society on technical applications.

The panel spent a great deal of time considering the impacts of terrorism and terrorist acts. It was felt that security issues surrounding the infrastructure of both the public and private sector would be something to be addressed at the forefront prior to Internet technology expanding its applications into law enforcement. In looking at the Cross Impact Analysis and listening to the discussions, it is apparent that Internet applications for law enforcement would be very positive. As an example, the expansion of Community Policing to include Technology Based Policing was seen as having broad positive implications.

Community and Technology Based Policing were described as being a help, as well as a hindrance to homeland security efforts. Law enforcement organizations at all levels could rely upon the Internet for immediate distribution of security and emergency preparedness information to its community members. Along these same lines, communities have a user-friendly means via the Internet to pass on information to law enforcement. However, the Office of Homeland Security could not rely upon this technology to reach all populations due to generational and social gaps, thus a duplicate communication system would also have to be in place.

On a local level, Community and Technology Based Policing were seen to have very positive applications in developing partnerships with local communities. Instant

messaging and video conferencing would allow field officers to receive instant communications from allied police and governmental agencies, as well as from local residents. Utilization of technology in this form would also create opportunities for the private sector to build upon the telematics industry and increase development of bandwidth for improved functionality and efficiency of the Internet. However, to make this a reality, partnerships must be formed with the private sector in an effort to properly plan for the future.

As previously mentioned, cyber terrorism and Internet security in general was seen as the link between success and setback of this technology. All of the identified trends would be significantly and negatively impacted. Homeland security efforts would be scrutinized for lack of security, planning, and protection to the infrastructure of the nation's communications capabilities. Applications and development of the technology would be subject to criticism if security lapses were to occur. To minimize this impact and create better opportunities for success, cyber security must be at the forefront for all stakeholders and preparations must be made during the continued development of Internet use and dependency.

Scenarios

In an effort to better understand the implications derived from the NGT analysis, the following scenarios were developed to provide a sense of realism for the future. The purpose of scenario planning is not to identify a specific future event, but rather to develop alternative scenarios. Scenarios are alternative descriptions of how the future might develop from an optimistic, pessimistic and normative or minimal change

standpoint. By preparing such scenarios, leaders and planners of the future can make better decisions today in preparation for the future.

Pessimistic Scenario – In the year 2007, law enforcement agencies across California, that have been under increasing demands to expand Community Policing via web or technology based policing, have found themselves back in the technological age of the 1990s. Hundreds of millions of dollars have been spent by the State of California since 2002, when a commitment was made by all of California's law enforcement agencies to equip themselves with wireless technology in a mobile environment. Over 400 police agencies in California have purchased or are ready to purchase equipment that will allow them to interact with any on-line public safety agency in the world via the law enforcement network created by the State of California.

This network was created as a result of the terrorist attacks from September 11, 2001, which highly criticized the sharing of information, or lack thereof, by law enforcement agencies. California had planned on using the Internet as its communications medium to link law enforcement agencies across California to share information. Funding for such an ambitious program came as the result of grants from public and private institutions, a 1/4 percent sales tax increase, and proportionate funding from each agency's general fund. Ford Motor Company also provided a large cost savings when it made Internet accessibility a standard feature in all of its cars in 2002. This plan was to become fully functional in 2008 after final tests were completed in law enforcement agencies currently pilot testing the system.

Selected public safety agencies from San Francisco to San Diego have been communicating with one another by sharing criminal history information and suspicious

activity reports with video and still pictures. They have also been conducting surveillance of highly populated areas using facial scanning software that alerts law enforcement to suspected criminal or terrorist activity. In addition to general criminal history and other database inquiries, agencies using this technology have also been communicating with their local residents directly from the field via e-mail, video technology, and instant messaging. This has allowed officers in the field to receive real-time information or updates directly from citizens, as well as the exchange of information. Patrol officers no longer need to drive to their stations or sub-stations to access law enforcement information, and thus patrol briefings are now held remotely from inside their patrol vehicles. The patrol vehicle became a true mobile office making public accessibility to the officers easier, while at the same time allowing officers to remain in the field.

Unfortunately, all of these plans came to a halt when an international terrorist organization worked in concert with domestic terrorists to hack into the State and Federal Department of Justice computer systems, including that of the FBI. After hacking into the system, the terrorists altered and deleted information of thousands of Californians DMV and criminal records. Some criminal history information has been deleted and many law-abiding California citizens now have a criminal history on record because of corrupted data entered into the system by the terrorists. In addition, law enforcement officials who have been pilot testing the Internet program have found that their computer has been corrupted by a system virus activated by the terrorists. As a result of this, privacy advocates have been granted an injunction halting the use of this technology, thereby keeping millions of dollars in hardware and software spread across the state from

being utilized. Law enforcement officers have been relegated back to under utilizing technology, while information sharing amongst law enforcement professionals, as well as citizens, has once again become scarce.

Optimistic Scenario - In the year 2007, law enforcement agencies across California, who have been under increasing demands to expand Community Policing via web or technology based policing, have found themselves leading the field of Community Policing. Hundreds of millions of dollars have been spent by the State of California since 2002 when a commitment was made by all of California's law enforcement agencies to equip themselves with wireless technology in a mobile environment. Over 500 law enforcement agencies in California have purchased equipment that will allow them to interact with any on-line public safety agency in the world via the law enforcement network created by the State of California.

This network was created as a result of the terrorist attacks from September 11, 2001. After action reports from the federal government and investigative media reports highly criticized the sharing of information, or lack thereof, by law enforcement agencies across America. California's plans on using the Internet as its communications medium to link law enforcement agencies across California to share information has now become a national model. Funding for such an ambitious program came as the result of grants from public and private institutions, a telecommunications surcharge, Internet taxation, and proportionate funding from each agency's general fund. Ford Motor Company also provided a large cost savings when it made Internet accessibility a standard feature in all cars in 2002. This, coupled with the decreased costs of hardware and software from the

computer generation heyday in the 1990s, has made what was once a mere concept a fully functional wireless communication system for California's 30,000 police officers.

Law enforcement agencies from the Oregon border to the Mexican border have been communicating with one another sharing criminal history information and suspicious activity reports with video and still pictures. Facial scanning software is being utilized for surveillance of highly populated areas for suspected criminal or terrorist activity. In addition to general criminal history and other database inquiries, these same officers can, at the click of a button, receive State approved training via video technology right in their patrol vehicles and can also provide court testimony from their patrol vehicles via video conferencing technology. Agencies using this technology have also been communicating with their local residents directly from the field via e-mail, video technology, and "instant messaging." This has allowed officers in the field to receive real-time information or updates directly from citizens who communicate from their home or business computer, thereby creating instant communication sharing, which had been highly criticized in past years.

As part of the state's Homeland Security efforts, all law enforcement agencies are networked into a central Records Management System and thus, share a massive database. This same database works in conjunction with the California Anti-Terrorism Information Center and Western States Information Center. All law enforcement agencies in the state can receive instant terrorism and security alerts and briefings directly into their patrol vehicles. The system provides for complete interoperability of all law enforcement agencies in the state. Patrol officers no longer need to drive to their stations or sub-stations to access or receive law enforcement information, and thus patrol

briefings are now held remotely from inside their patrol vehicles. The patrol vehicle has become a true mobile office making public accessibility to the officers easier, while at the same time allowing officers to remain in the field.

All of these plans and investments could have come to a halt when an international terrorist organization worked in concert with domestic terrorists to hack into the Department of Justice (DOJ) computer systems, including that of the FBI. Fortunately, significant efforts were made by many agencies, both private and public, to safeguard the security and privacy of the system. The Internet security technology developed to safeguard DOJ databases against terrorist activity was now turned around and used as a tool to hunt down and capture those terrorists who attempted to hack into the databases. Using special mobile security technology, local law enforcement officials quickly apprehended the domestic and international terrorists using the mobile technology that was being targeted for terrorist attacks.

Normative Scenario - In the year 2007, law enforcement agencies across California, who have been under increasing demands to expand Community Policing via web or technology based policing, have found themselves still striving to meet these demands. Plans to spend hundreds of millions of dollars by the State of California since 2002, when a commitment was made by all of California's law enforcement agencies to equip themselves with wireless technology in a mobile environment, has progressed at a slower pace than expected. Over 400 police agencies in California still need to purchase equipment that will allow them to interact with any on-line public safety agency in the world via the law enforcement network planned by the State of California.

This network was created as a result of the terrorist attacks from September 11, 2001. After action reports from the federal government and investigative media reports highly criticized the sharing of information, or lack thereof, by law enforcement agencies across America. California's plan to use the Internet as its communications medium linking law enforcement agencies across California would have been a national model, however the delay has allowed other states to begin their own state law enforcement networks. Funding for such an ambitious program has been slow to come from public and private institutions and a 1/4-cent sales tax increase failed with the voters. Ford Motor Company provided a large cost savings when it made Internet accessibility a standard feature in all cars in 2002, but the long-term Internet and cellular service fees have created budgetary dilemmas for some of California's smaller law enforcement agencies. Although the hardware and software for such a project has been made affordable to most, newer technology has been developed making the affordable systems virtually obsolete.

Law enforcement agencies from the Oregon border to the Mexican border could have communicated with one another sharing criminal history information, suspicious activity reports with video and still pictures, and conducting surveillance of highly populated areas using facial scanning software that could alert law enforcement to suspected criminal or terrorist activity. In addition to general criminal history and other database inquiries, these same officers could have, at the click of a button, received state approved training via video technology right in their patrol vehicles and could also have provided court testimony from their patrol vehicles via video conferencing technology. Agencies had also planned on using Internet technology to communicate with local

residents directly from the field via e-mail, video technology, and instant messaging. This would have allowed officers in the field to receive real-time information or updates directly from citizens who could communicate from their home or business computer, creating instant communication. Patrol officers must continue to drive to their stations or sub-stations to access or receive law enforcement information and continue with traditional patrol briefings at the beginning of their shift as opposed to remote Internet briefings from the field. Accessibility to the public remains static.

All of these plans remain just that…plans, until public and private officials develop security plans and mediate privacy issues still being reviewed by the court system. Law enforcement officials continue to utilize the Internet with limited applications from office desktops and cellular phones, while only a few California agencies are experimenting on their own with Internet access and related functionalities from a mobile computing environment.

The purpose of scenario planning is not to pinpoint future events, but to highlight large-scale forces that push the future in different directions. It is about making these forces visible, so that if they do happen, the planner will at least recognize them. It is about helping make better decisions today.[14] This planning process allows us to create strategic plans so that we can manage change more effectively. The following chapter will highlight a strategic plan and its various components as it applies to the issue of the Internet in a mobile computing environment.

CHAPTER THREE

STRATEGIC PLAN

Strategic Planning

Due to constant changes in society, at some point we find ourselves adjusting lifestyles to meet this change. These changes can be something as simple as a change in clothing and hairstyles, or as complicated as changes in the various forms of technology used in daily activities. These changes, however, do not occur overnight and require some foresight and proper planning. Failing to adjust, adapt, or plan for such change can result in conflict in both personal and professional experiences.

Taking this same analogy and applying it to one's workplace requires organizations to also strategically plan for their future. A strategic plan is a "structured approach, sometimes rational and other times not, bringing anticipation of the future to bear on today's decision."[15] This requires organizations to periodically examine their mission and values, which include organizational goals, and consider how the organization will accomplish its vision. "Successful strategic planning leads to action, builds a shared vision that is values-based, is an inclusive participatory process in which employees take on a shared ownership, accepting accountability to the community, is externally focused and sensitive to the organization's environment, is based on quality data, requires an openness to questioning the status quo, and is a key part of effective management."[16]

This chapter will focus upon various components of strategic planning as it applies to the issue of the use of the Internet in a mobile computing environment. Using the Optimistic Scenario in Chapter Two as a vision for the future and guideline for

strategic planning, it is imperative to conduct a situational analysis of the organization's environment as it strives to develop various strategies. The very definition of strategic planning stresses the importance of focusing on the future within the context of an ever-changing environment – the myriad of political, economic, social, technological, demographic, and legal forces that change the world daily. Skill at assessing the environment and then being proactive in responding to that environment determines who is effective in using their resources and, ultimately, who survives.[17] The analysis in the following pages will examine the weaknesses, opportunities, threats, and strengths underlying planning for the vision from the Optimistic Scenario, as well as a stakeholder analysis and development of strategies. Such a planning process will allow for the development of a strategic plan in creating statewide interoperability of law enforcement patrol functions via the Internet from a mobile computing environment.

Situation Analyses – What are the organizational weaknesses underlying planning?

- Law enforcement has been slow to adopt broad-based technology into its mission. Being slow in this realm has been detrimental to the growth and development of both personnel and technology itself. When technology is introduced, it is often done so with application and use towards some field other than law enforcement. As such, law enforcement is by its very nature one step behind the generation of new technology. On the other hand, when technology is developed for law enforcement, the profession has been slow in its adoption, implementation, and commitment.

- Employees do not have the skills, knowledge, or training to commit themselves to the application of the technology. Technology is an expertise all its own that requires recruitment and retention of personnel interested in the field. The failures of various technologies have been attributed to the forcing of individuals like line-level police officers into fields for which they have no background, technological expertise, interest or aptitude.
- Police organizations lack the infrastructure and funding to support large technology projects. Smaller organizations are significantly impacted due to limited funding and technical support.
- Generational differences between various leaders within organizations creates a division, thus slowing the process towards change.

What are the external opportunities underlying planning?

- The very unfortunate circumstances surrounding the terrorist attacks against the United States on September 11, 2001 brought with it heightened awareness of homeland security. Local law enforcement has been tasked to take on a greater role in homeland security efforts. As a result, the need for technology expansion to all of local law enforcement is much more intensified and justified.
- Homeland security efforts have identified the need for law enforcement agencies across the United States to improve communications and interoperability of communications systems. Information sharing in a timely manner will be critical to the success of future law enforcement communication technologies.

- Funding from such sources as the Local Law Enforcement Block grant, High Technology grant and Citizens Option for Public Safety grant may allow for the creation of a national or local infrastructure of communications technology.
- Already existing partnerships between private sector companies, nonprofit agencies, and schools of higher learning that research technological applications may be used to research law enforcement applications.
- The State of California's Office of Emergency Services Mutual Aid Plans and Standardized Emergency Management System, and the California Department of Justice's California Anti-Terrorism Information Center, California Law Enforcement Telecommunications System, and Western States Information Network provide an already existing model for information sharing.
- The increasing use of the Internet as a tool to commit crimes, as well as investigate crimes may lead to the development of additional means of solving crimes in a timelier manner.
- Societal demands placed upon law enforcement agencies to expand and include Technology Based Policing into Community Oriented Policing will create opportunities for the advancement of Internet technology.

What are the external threats underlying planning?

- Cyber terrorism and related security issues create significant challenges to the utilization of the Internet as a means of secure communications for law enforcement.

- Funding demands and differences of opinion in regards to funding methods will challenge project development. Smaller agencies may lack any funding, while larger agencies may be unwilling to share costs.
- Struggles over control of the system, its infrastructure, policies, and procedures may require the development of a regional effort or special agency comprised of representatives of involved agencies.
- The bureaucratic process of obtaining agreements and Memorandums of Understanding from all involved agencies may ultimately lead to legal challenges.
- Some law enforcement agencies will be unwilling to share information, while special interest groups may challenge privacy rights.

What are the internal strengths underlying planning?

- Law enforcement organizations, for the most part, are accustomed to working within groups and flexible enough to adapt to changes to the system.
- Law enforcement organizations have traditionally received funding based on articulated needs and demands for public safety reasons.
- Law enforcement organizations have been successful lobbying local legislators for the development of public safety programs.
- Law enforcement organizations have existing information networks and plans to disseminate sensitive information.
- Law enforcement organizations are currently developing infrastructures to support basic Internet access and other information-sharing technology.

- The next generation of police recruits are entering the profession with computer and Internet use backgrounds.

Stakeholder and Snail Darter Analysis

Stakeholders are groups or individuals who are affected by, or can influence a decision or action and as such, play a significant role in success or failure. Unfortunately, too many actions are attempted without input from stakeholders, who often have differing opinions, values, concerns, and ideas regarding an issue. When issues are overlooked or not addressed, delays often occur as project development is slowed due to the need to address or include a stakeholders viewpoint. Such delays are often referred to as "snail darters," as they are unforeseen or overlooked obstacles. A snail darter may be an individual stakeholder, an event, or process that had been overlooked, ignored, or unforeseen. By conducting a stakeholder analysis, whereby a collection of a wide variety of perceptions is gathered, delays and failures can be minimized, while contributing to the success of the project. The following are identified stakeholders and snail darters for this issue:

- Police Leaders - Law enforcement leaders in support of the project, this being the optimistic scenario previously discussed, will be proactive in developing strategies, plans, funding, legislation, and partnerships towards a successful outcome. Law enforcement leaders who do not support such an endeavor for reasons such as financial, generational, or values can create challenges due to the need for industry-wide support to create a successful interoperability project.

- Employee Unions – Employee unions representing such groups as police officers, supervisors, dispatchers, and civilian employees may address concerns over the need for additional training, the need for additional personnel due to increased workload and expectations, resistance to the project for similar reasons to that of the non-supporting police leaders, and resistance to the expansion of Community Oriented Policing to Technology Based Policing.
- Community Members – Community members will come in three forms: in favor, non-supportive, or non-committal. Those in favor will support the expansion of such areas as Community Policing, the increased community information sharing and sense of security with a new operational tool. Those non-supportive will be critical of the associated costs, question the applicability of local law enforcement to homeland security, and question the overall applicability of Internet use. Those non-committal are a silent force that could be susceptible to the popular opinion.
- Department of Justice – The Department of Justice at both the state and federal levels will play a critical role in the development and on-going maintenance of such a project. It would seem that the California Department of Justice would be the administrator of the program just as they are for other statewide initiatives like the 9-1-1 System and California Law Enforcement Telecommunications System. The Federal Department of Justice would be a critical link for information regarding Homeland Security and other databases. Due to financial obligations, one or both of these entities may push for the other to absorb costs or overall responsibility.

- Office of Homeland Security – Both the state and federal governments maintain an Office of Homeland Security and both stand to benefit from the development of such a project. However, one or the other may not desire the responsibility.
- Allied Agencies – Depending on financial obligations and current technological infrastructure, various agencies throughout the state may not be equipped to either pay for such a project or have the necessary infrastructure in place to complete the project (i.e., cellular signals for mobile Internet use), especially in smaller rural communities.
- Internet Service Provider's (ISP's) and Telecommunication Companies - ISP's and telecommunication companies should see a large increase in revenue from monthly service charges and other costs. The development of a secured site for law enforcement may not be a feasible financial endeavor for the private sector.
- Information Systems Personnel (External and Internal) – Information Systems personnel both internal and external to organizations will question security of such an endeavor. Private industry security groups may advocate that security systems in existence are sufficient, while those charged with securing internal organizational systems may argue otherwise.
- Elected Officials - Elected officials at all levels will be asked to develop and support such a project. The project will require financial support from all levels, including the possibility of increased or diverted taxes. Various groups will support the need for public safety, while others will question the costs and need, especially in smaller rural communities.

- Federal Bureau of Investigation (FBI) – The FBI has been a fixture in American society as the nation's premiere law enforcement agency. This fixture has also placed upon it a sense of secrecy even to local law enforcement. Due to the nature of its sensitive investigations, information sharing has been limited to only those within the FBI. Sharing of such information for homeland security efforts via the Internet to local law enforcement, let alone via traditional means, will be a challenge.
- California Peace Officers Standards & Training (POST) – POST may utilize the technology to expand training opportunities to officers via the Internet.
- California Court System – The California court system may find video conferencing to be a viable alternative to in-person testimony.
- Special Interest Groups – Special interest groups like the American Civil Liberties Union, taxpayer reform groups, and police reform groups will question privacy issues, police abuse of the system, and will stress the need for less government intrusion.

Strategies

Strategy development follows the creation and affirmation of the organization's purpose statement, environmental and program data collection and analysis, and identification of critical issues. Strategy formulation is a combination of rational, scientific examinations and educated, intuitive decisions that entail:

- Examining the organization's critical issues

- Determining how the organization's strengths and skills can be employed to address the critical issues
- Analyzing opportunities and strengths and looking for ways to synthesize the two
- Exploring and choosing the best approaches for the organization.[18]

The following are broad based strategies intended to move law enforcement organizations toward the vision created by the optimistic scenario:

Strategy #1 – Formation of Research and Development teams to focus on critical issues identified in the various analyses. These teams should consider stakeholder and snail darter analysis to prepare for the future development of a strategic plan.

Strategy #2 – Given a mission, vision, and set of values, private industry technology groups should prepare a Request For Information (RFI) to assist government in assessing impacts to project development. These impacts could be social, technological, environmental, economic, and political, which will help planning groups address various needs.

Strategy #3 – A regional group or county should implement an abbreviated program to assess the successes and shortcomings. Results from this test market would be included in a statewide proposal and would also address any impacts identified by the private industry RFI.

Strategy #4 – Elected state officials should be introduced to the previous three strategies to form their own committees and to seek input and direction from their constituents.

The following chapter will focus on the transition of a strategic plan to reality. Various components of transition management and implementation will be discussed.

CHAPTER FOUR

TRANSITION MANAGEMENT

Transition Management – Commitment Planning

Change within organizations require well thought out planning, in as much detail as does issue development, historical development, research, and forecasting. Part of the planning for change requires a transition management plan to address issues of stakeholder involvement, commitment planning, implementation planning, and development of an evaluation process. Having such a transition management plan will aid the evolutionary process of change by addressing such issues as organizational resistance, assignments of responsibility, and actions for securing stakeholder support. A transition management plan will help prepare the organization for change or mitigate the impact of change.

In any complex change process, there is a critical mass of individuals or groups whose active commitment is necessary to provide the energy for the change to occur.[19] The critical mass are those people in an organization who are necessary to create change. It could be members of an executive and supervisory team, members of the police union, members of a police commission and so forth. As part of a stakeholder analysis, this critical mass must be identified and a strategy developed to obtain some degree of commitment. One such strategy is that of a commitment plan. "A commitment plan is a strategy, described in a series of action steps, devised to secure the support of those subsystems, which are vital to the change effort. The steps in developing a commitment plan are:

1. Identify target individuals or groups whose commitment is needed.
2. Define the critical mass needed to ensure the effectiveness of the change.
3. Develop a plan for getting the commitment of the critical mass.
4. Create a monitoring system to assess the progress."[20]

The stakeholder and snail darter analysis discussed in the previous chapter provides a starting point for such a commitment plan. The identified stakeholders and snail darters are those whose commitment is needed and who make up part of the critical mass. The critical mass can be narrowed down to those individuals who by virtue of their title, position, or level of expertise have the authority to make decisions for a larger group. For example, a commitment will be needed from individuals and groups who are comprised of law enforcement leaders, employee unions, community members, the Department of Justice, the Office of Homeland Security, elected officials, special interest groups and so forth. The critical mass may include representatives from each of these groups who also have the ability and authority to make decisions regarding the issue. They may include individual Police Chiefs and Sheriffs, Union Presidents, Mayors, community activists and other leaders of organizations.

Once the target group and critical mass have been identified a plan to gain commitment must be developed. No project or plan has been implemented without some level of resistance. Where resistance exists, it is necessary to work with it and honor it, but also to find ways to neutralize it for short periods so that the resister can hear a different perspective on the problem. "The following intervention strategies can help overcome resistance: persuasion, problem finding and resolution, educational intervention, resistance management, role modeling, changing reward systems, and

forced collaboration."[21] Each strategy should be evaluated and monitored for each set of circumstances to assess progress.

Once a commitment plan has been established, role relationships should be identified to assist in project implementation and related decision-making authority. This can be accomplished through a mechanism called Responsibility Charting. In essence, Responsibility Charting involves the identification of various stakeholders within the project, identification of various decisions or actions to be completed, and finally, each person's role in decision-making. Roles should be classified in the following manner:

1. Responsibility to ensure that decisions or actions occur
2. Approval of actions or decisions with the right to veto
3. Support of actions or decisions by provision or resources with no right to veto
4. Informed of actions or decisions with no right to veto.[22]

The following is a simple example of Responsibility Charting:

Project: Internet implementation into patrol vehicles

Action: Selection of mobile computer equipment

R = Responsibility; A= Approval; S = Support; I = Informed

Project Manager:	R, A
Police Chief:	A
Police Managers:	S
Police Supervisors:	S
Police Officers:	I
Police Union:	S, I
Technicians:	S, I

Such assignment of roles and responsibilities help provide for a managed transition and limit ambiguity in the implementation process.

Implementation

The following is a proposed and abbreviated implementation plan considering the processes of a stakeholder analyses, commitment planning, responsibility charting, and the previously discussed strategies:

Utilizing the works of this futures study, with an emphasis on its mission, values, and vision, a pro-active and contemporary Police Chief or Sheriff must personally adopt it for presentation to the critical masses and stakeholders. Presentations must be made to professional organizations such as the California Police Chief and Sheriff's Association, the California Peace Officers Association, and the Peace Officers Research Association of California to obtain support for continued research and development of the project. This would be the first step in dealing with stakeholders and would address various questions and issues and may require repeat presentations to allow time for additional research prior to votes of support or non-support.

Assuming support is granted for additional research, a team of individuals from each association should be developed to conduct additional research and should also include representatives from other stakeholder groups such as the Department of Justice, Special Interest Groups, and Community Members. It would also be recommended that a Nominal Group Technique (NGT) be used to solicit a variety of opinions and thoughts on the issue to be included in the strategic plan. The strategic plan should also identify the various roles and responsibilities of individuals and teams.

Given a mission, vision, and set of values, private industry technology groups should be solicited to prepare a Request for Information (RFI) to assist government in assessing impacts to project development. These impacts could be social, technological, environmental, economic, and political, which will help planning groups address various needs. Information from the RFI's should be included in the strategic plan.

Once the strategic plan has been revised with the RFI's, a partnership should be formed with private industry groups to address such issues as security, implementation, costs, and other identified issues, as well as future development plans for the technology. This partnership should develop the final draft of the Strategic Plan and be presented to the critical mass for approval. The mentioned partnership should be maintained as a standing committee to one or all of the associations for continued development of technology plans.

A regional group of law enforcement organizations or a selected county should implement an abbreviated program to assess the successes and shortcomings. Results from this test market would be included in a statewide proposal and would address any impacts identified in the RFI or Strategic Plan.

A detailed strategic plan should be brought to an elected state official for additional research and development prior to introduction of legislation requiring implementation of this statewide wireless information network.

Organizations, whether small or large, must make a commitment at the onset to follow through with implementation plans. The original strategic plan may be adopted in full, partially, or not at all, but it is incumbent on local leaders, which make up the critical

mass, to maintain a united front and continue its efforts towards its mission, values, and vision.

The following chapter will summarize the finding of the previous chapters and describe various implications, as well as recommendations for action.

CHAPTER FIVE

FINDINGS AND CONCLUSIONS

The Internet is a tool that is still developing and finding its place and use within the law enforcement profession. However, just as the telephone was once a new technology and developed into an important tool for law enforcement, society and the police profession should be prepared to use the Internet as a developing tool for the future. The complex network of existing telephone lines and cellular signals that traverse the state is a mode of communication awaiting expansion by leaders and change agents willing to step forward and champion a cause. The cause to be championed is that of expanding existing wireless and Internet technologies into the line level patrol functions of law enforcement agencies across the state. Both of these technologies have come too far to not explore future uses and applications.

Given the current state of affairs on homeland security, the identified needs of law enforcement interoperability and information sharing, and the ever-increasing need of creating additional lines of communications with community members, law enforcement must take advantage of the circumstances. Looking back at the trends and events developed during the NGT process, as well as the implications developed from strategic planning and transition management planning, it is ever more convincing of the need to utilize Internet applications in a patrol environment.

The optimistic scenario presented in chapter two provides a microscopic realization and answer to the issue question, “How will the use of the Internet in a Mobile Computing Environment Change the Patrol Function in Law Enforcement Agencies by 2007?” The list of applicabilities are endless and would include such functions as, instant

messaging across the state to any in-service patrol vehicle, instant homeland security alerts from California's Anti-Terrorism Information Center, instant communications to community members, access to law enforcement references and databases, website links to public and private agencies, integrated Records Management Systems, video technology, and more. The patrol function will, in fact, change for the good with increased efficiency and proficiency of police practices, including Community Policing, better coordination of police resources, and increased access to information. However, a good plan is not without challenges. Law enforcement agencies must prepare controls and auditing systems for Internet access abuse, monitor over- dependency on technology to avoid a decrease in human socialization, and invest in system and infrastructure security to mitigate anticipated challenges.

During the time that this concept develops into reality, law enforcement organizations must promote themselves so that they receive consideration for technology development. Unfortunately, for many years, law enforcement has been on the user end of technology as opposed to the research and development end. Take, for example, the creation and expansion of the Internet. It was originally developed for use as a network for colleges and universities, but expanded into private enterprise after research by private sector entrepreneurs. Had law enforcement been on the leading edge of such development, its use and applicability for law enforcement might be completely different today. The culture of law enforcement must also change to encourage this type of involvement with research and development. One such opportunity for involvement is with the Net21 state research facility at the University of California, Berkeley. Net21was recently created with private and public funding to design and shape the future of the

Internet with advanced applications. It is incumbent upon law enforcement leaders to insure law enforcement representation.

A responsibility for law enforcement leaders does end here though. There must be legislative involvement pressing for system-wide advancements in broadband technology and regulations of the Internet. Broadband technology will allow for the seamless transmission of video and other large pieces of data without delay and will provide for a wide array of applications for law enforcement. Regulations of the Internet would include such things as: cost controls for the poor and disadvantaged, broadband mandates for all households, and demands for increased security features. Included in such regulations would be the loosening of restrictions on law enforcement seeking access to Internet communications during cyber crime investigations.

One of the biggest political challenges facing leaders attempting to lobby this initiative will be budgetary and other financial considerations. It is unrealistic to work off of a premise that all of the 500 or so law enforcement agencies in California will voluntarily agree to purchase mobile data computers, mounts and other hardware, wireless services, related software, on-going maintenance, training, and so on. Mandates placed upon law enforcement via state legislation to implement such a program will create a large financial obligation to the State of California, but it is the most logical option considering the magnitude of the project and oversight needed for implementation and administration. However, such a project is feasible and has been done in the past on a similar scale.

Comparing this project to that of the statewide 9-1-1 system implementation of the early 1980s reveals similar demands and challenges. The 9-1-1 system has been

partially funded via the Emergency Telephone Users' Surcharge, or 9-1-1 tax, imposed by the Public Utilities Commission on all telephone services, including wireless services. Considering an amendment to this tax to include funding for a statewide law enforcement communications program via the Internet may be a political challenge at all levels due to society's current opinion of "no new taxes." One other taxation option would be for the lobbying of an Internet tax dedicated specifically for statewide law enforcement efforts. Currently, California has no taxes on the Internet as a result of California's Internet Tax Freedom Act, which precludes taxation of Internet access.

At the local level, shared funding should be considered via Local Law Enforcement Block Grants, Citizens Option for Public Safety (COPS) grant monies, and High Technology grant monies. Legislation may be required for a one-time dedication of these funds for infrastructure development at the local levels.

As can be seen, there are hosts of logistical, financial, political, and management challenges for such an endeavor as detailed throughout this project. However, it is not something outside the realm of possibility when compared to such other endeavors as the 9-1-1 system. In some facets, this project may be more manageable for implementation due to technological infrastructures already in place.

It is recommended that the California Police Chief and Sheriff's Association take the lead in introducing any proposal to the industry utilizing the strategies and transition plans discussed earlier. Taking such a lead must also follow with a commitment plan, responsibility charting, timelines, and progress reports to the association to help with follow through and evaluation of progress.

Law enforcement leaders must be able to set a vision for the future and be willing to take certain risks to achieve that vision. Walt Disney, founder of the entertainment giant Disney, had the credo: "I dream, I test my dreams against my beliefs, I dare to take risks, and I execute my vision to make those dreams come true."[23] Any successful organization must stay close to its values, mission, and vision to be the driving force, as it was with Disney. Just as Disney was a dreamer who applied his dreams to his beliefs, followed by execution of those beliefs, law enforcement organizations must do the same. This can be applied by leaders of organizations and associations having a vision, testing that vision with personal and organizational values, and the willingness to take calculated risks to see the vision come true. Unfortunately, it is the lack of creative visions and risk taking that many times limits the potential success of an organization or the profession. Organizations must be willing to test areas of this profession that have not been tested before. This will only come from those creative, visionary police leaders who are willing to, "dream, believe, dare, and do" those things that have never been done before.[24]

APPENDIX A

List of Trends

1. Level of Homeland security
2. Use of “Instant Messaging” and video conferencing
3. Use of Telematics technology
4. Capacity of bandwidth technology
5. Amount of Internet terrorism acts
6. On-line commerce and banking
7. Privacy issues will be challenged by civil advocacy groups
8. Use of GPS technology will continue to expand
9. Level of miniaturization of computers and other hardware
10. “Gaming” technology toward simulation/interactive training
11. Dependency upon the Internet for product upgrades
12. Affordability of hardware and software
13. Security concerns
14. Use of law enforcement web sites
15. The rate of increase of Internet users
16. Planned computer networked neighborhoods
17. “E911” implementation
18. The number of Internet users
19. Use of satellite communication technology
20. Amount of information via Internet (i.e. secure website technology, Megan’s Law, etc.)
21. On-line learning and training

APPENDIX B

List of Events

1. Telephones, televisions, VCR's appliances and other electronic equipment are replaced by Internet controlled computer-aided systems.

2. First police agency implements Technology Based Policing.

3. Legislation enacted regulating use of the Internet.

4. Cyber terrorists hack into the DOJ/NCIC/DMV, etc. computer system creating a denial of service to users, as well as changing and/or deleting of criminal history information.

5. The increased use of video and other camera technology will results in the first capture of criminals and terrorists.

6. Continued wars in Afghanistan, Iraq, and other Middle Eastern countries with the United States will make more readily available high-tech crime-fighting technology after it is field-tested in war.

7. Terrorist attacks on communication towers/facilities will incapacitate law enforcement communication systems.

8. Misuse and abuses of the Internet to access classified information by police officers and civilian personnel will result in increased disciplinary cases and civil rights abuse allegations.

9. Y2K type law enforcement planning will be the norm, but allied law enforcement agencies will be networked to the Internet to share information from the field using Mobile Data Terminals and cameras.

10. Political in fighting over who controls the network will slow the progress of utilization of this technology.

11. Terrorist attacks will require better technology for law enforcement, as well as the need for information sharing between local, state, and federal agencies.

12. Standard equipment in all cars will be Internet equipped, pushing law enforcement to utilize the equipment and allowing officers to communicate with vehicles on the road utilizing license plates as the e-mail address.

13. Natural disasters will occur, disabling law enforcement communications technology. This would also include such things as meteor showers that disable satellite technology.

14. Demands by the Generation X'ers will require the implementation of Internet technology, as they will have the knowledge to operate and expand the technology.

15. Roll call briefings will become automated utilizing e-mail, instant messaging, and video conferencing to police officers in the field.

16. High-profile child abduction cases like Polly Klass and "Megan" will push for information to be readily available to law enforcement.

ENDNOTES

[1] California Peace Officer Standards and Training (POST), Employment Data Statistics, 1990.

[2] Telecompetition, Inc., "Third World Wireless Coming Fast – Study," Hhttp://www.cellular.co.za/H, July 2001

[3] Genaro C. Armas, "Net Access Increases in U.S. Homes," The Union-Tribune, September 11, 2001, 2.

[4] Geri Lama, Hhttp://www.onstar.com/H, November 12, 2001.

[5] Andrew Seybold Group LLC, "Wingcast: Driving Telematics in New Directions," White Paper, March 2001.

[6] Knowledge Corner, "About 3G-Third Generation Wireless Systems," Hhttp://www.info.gov/H

[7] Andrew Seybold Group LLC, op.cit.

[8] Nokia Inc., "What is 3G," Hhttp://www.nokia.com/H

[9] The Futurist, "Outlook 2002," November-December 2001, Page 3

[10] The Futurist, "The Mission of the Futurist," July-August 2001, Page 1

[11] Andrew Seybold Group LLC, op.cit.

[12] Ibid.

[13] Gene Stephens, P.O.S.T. Command College Session I, "Examining the 21st Century in Search of Challenges and Opportunities for Law Enforcement", May 9, 2001.

[14] Lawrence Wilkinson, "How to Build Scenarios," Wired Ventures, 1995, 3.

[15] Tom Esensten, Organizational Effectiveness Consulting, P.O.S.T. Command College Session VI, "Strategic Planning", March 18, 2002.

[16] Alliance for Nonprofit Management, "Strategic Planning," Hhttp://www.allianceonline.org/H

[17] Alliance for Nonprofit Management, "Situation Assessment," H http://www.allianceonline.org/ H

[18] Alliance for Nonprofit Management, "What is a Strategy and how do we develop one?," http://www.allianceonline.org/

[19] Reuben T. Harris & Richard Beckhard, Organizational Transitions: Managing Complex Change, Addison-Wesley Publishing Company, 1987, Pg. 92.

[20] Ibid., 93.

[21] Ibid.

[22] Ibid.

[23] Capodagli, Bill & Lynn Jackson, "The Disney Way," McGraw Hill, 1999, 1.

[24] Ibid.

Bibliography

Capodagli and Jackson, Lynn. The Disney Way. New York: McGraw-Hill, 1999.

Horrigan, John B. "Cities Online: Urban Development and the Internet," Pew Internet & American Life Project, 2001.

Hoyle, John R. Leadership and Futuring. Thousand Oaks: Corwin Press, 1995.

Hunter, Ronald ., Mayhall, Pamela D., and Barker, Thomas. Police-Community Relations. New Jersey: Prentice Hall, 2000.

Johnston, Richard L. "The National Cybercrime Training Partnership," The Police Chief, 69, no. 1 (January 2002): 52.

Kouzes, James M., and Posner, Barry Z. The Leadership Challenge. San Francisco: Jossey-Bass, 1995.

Lindblom, Charles E. The Policy Making Process. New Jersey: Prentice Hall, 1980.

Levy, Steven. "Living in a Wireless World," Newsweek, December 10, 2001, 57.

Maran, Ruth, Internet and the World Wide Web Simplified. Foster City: IDG Books, 1995.

Police Executive Research Forum. "Police Management: Issues & Perspectives." Sam Houston State University, 2001.

Report on the Telecommunications and Information Technology Gap in America. Falling through the Net: Defining the Digital Divide. U.S. Department of Commerce, 1999.

Roberts, Steven. "Domestic Security," Journal of Counterterrorism & Homeland Security, Vol. 8, No. 2, 2002.

Rogers, Donna. "On the Road Again," Law Enforcement Technology, 29, no. 1 (January 2002): 58

Rost, Joseph C. Leadership for the Twenty-First Century. Westport: Praeger, 1993.