HOW WILL EMERGING TECHNOLOGIES BE USED BY A MID-SIZE URBAN LAW ENFORCEMENT AGENCY TO ADDRESS WIRELESS DATA TRANSMISSION NEEDS BY 2009?

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

By

Lieutenant Mark Senkle
Pleasanton Police Department

Command College Class XXXVI

Sacramento, California

September 2004

36-0720

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: crating it, constraining it, adapting to it. A futures study points the way.

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

Copyright 2004
California Commission on Peace Officer Standards and Training

TABLE OF CONTENTS

LIST OF TABLES iv

Chapter I

ISSUE IDENTIFICATION 1

Introduction 1

Commercial Wireless Networks 4

First Generation 5

Second Generation 5

Evolution Path (2.5G) 6

Third Generation 7

Fourth Generation 9

Private Data Network 11

Private Radio 11

WiFi 11

WirelessMAN 13

Satellite Data Networks 14

Future Applications 14

Streaming Video 15

Internet Protocol Based Applications 16

Personal Data Device Applications 17

Summary 17

Chapter II

FUTURES STUDY 19

Nominal Group Technique 19

Process 19

Trend Analysis 20

Event Analysis 27

Cross Impact Analysis 32

Alternative Future Scenarios 34
Scenario 1: Pessimistic 35
Scenario 2: Normative 37
Scenario 3: Optimistic 39
Planning for the Future 41

Chapter III
STRATEGIC PLANNING 42
Introduction 42
Organizational Description 42
Vision 43
Goals 44
Organizational Analysis 45
Internal Weaknesses 45
External Weaknesses 45
External Threats 45
Internal Threats 46
Stakeholder Identification and Analysis 46
Development of Alternative Strategies 50
Preferred Strategy 53
Implementation Plan 54

Chapter IV
TRANSITION MANAGEMENT 58
Change Process 58
Commitment Planning 58
Commitment Charting 59
Strategies for Getting Commitment 60
Responsibility Charting 62
Evaluating Success 65

Chapter V
CONLUSIONS AND RECOMMENDATIONS 67
Review 67
Recommendations 69
Navigating the Wireless Nightmare 71

APPENDIX I (NGT Group) 74

APPENDIX II (NGT Events List) 75

APPENDIX III (NGT Trends List) 76

ENDNOTES 77

BIBLIOGRAPHY 81

LIST OF TABLES

Tables		Page
2-1	Trend Summary	21
2-2	Event Summary	29
2-3	Cross Impact Analysis	33
4-1	Critical Mass Commitment Chart	60
4-2	Responsibility Chart	65

CHAPTER I
ISSUE IDENTIFICATION

Introduction

The worldwide market for wireless communications has enjoyed tremendous growth over the past three decades. Wireless technology is now capable of reaching hundreds of millions of people at virtually every location on the face of the earth. With the tremendous success of wireless messaging services, it is not surprising that wireless data communication is being applied in the business and government realm.[i]

Employing a mobile field work force, law enforcement has long recognized the need to provide information to field personnel in a timely and efficient manner. In the mid to late 1970s law enforcement technology pioneers began using short text messaging via private radio data systems. These data networks are slow, 4.3mbs to 9.6mbs. The networks enabled mainframe computers to send short text messaging to mobile terminals. The availability of software applications was very limited. Initially these systems allowed computer aided dispatch systems to send limited call information and BOLO's (Be On the Look Out) to patrol cars. With the advent of standardized Internet Protocols (TCPIP), software advances and integration with criminal justice databases, these systems began to provide field personnel with relatively quick access to criminal and vehicle databases.[ii]

With the advent of personal computers, powerful servers and improved data networks, law enforcement has enjoyed a proliferation of software applications providing better access to data and improved work processes. Modern law enforcement agencies enjoy field access to integrated computer aided dispatch, records management, criminal justice databases, vehicle license databases and field reporting. A number of agencies are

currently using their wireless networks to provide mapping and automated vehicle location using the Global Positioning System. A few law enforcement agencies have recently experimented with wireless access to Internet applications such as California's system which allows law enforcement to access Department of Motor Vehicle photographs through the Internet.[iii]

Most agencies using wireless data networks have upgraded their hardware to include personal computers installed in their operation's vehicles. This has allowed agencies to take advantage of modern software applications in the vehicle and on their networks. Many of these applications require significantly more bandwidth than their predecessors that were designed to function on the low bandwidth networks provided by law enforcement's private radio networks. Agencies that are still using these low bandwidth wireless networks are restricted in their ability to implement new wireless applications. Over the past three or four years, a number of agencies migrated to cell analog and digital wireless technologies. These technologies were introduced by commercial service providers and were developed for the fast growing commercial wireless data market. These networks provided law enforcement with a number of desired benefits. They were wide area networks, had minimal initial investment costs and at bandwidths as high as 19kbs they were more than twice as fast as the radio data networks of the time. These faster wireless networks allowed law enforcement to implement more bandwidth intensive applications. The availability of the faster networks has also driven the development of wireless applications and interest in the potential of wireless applications.[iv]

Based on literature review, lectures and discussions with field experts the following is a list of the major forces driving law enforcement to upgrade their wireless networks:

- Agencies are being forced to upgrade their networks as vendors stop supporting old technology and begin to force agencies into newer technology that is less expensive for vendors to support and provides higher profits.
- Law enforcement is a minor player in the wireless data market and therefore does not drive the technology changes.
- It will be necessary for law enforcement to take advantage of market and technology changes to benefit their needs.
- Society's demand on law enforcement to increase service and performance will continue to drive the use of technology.
- The development of hardware and software will drive law enforcement to develop and implement supporting network backbones including wireless technologies.
- Law enforcement agencies will need to continue to meet government standards for the security of transmitted criminal justice information.
- International and domestic terrorism has created a push for law enforcement agencies to transition to protocols that will support interoperability between government agencies.

Over the next few years, most law enforcement agencies will take on the task of planning and implementing wireless technologies for their agencies. The backbone of these projects will be the wireless and wired data networks needed to support the access

to and sharing of data. The decisions agencies are making today will determine how emerging technologies will be used to address wireless data transmission needs over the next five years. These decisions will directly impact their ability to implement new hardware and software technologies over the next five to ten years. It is critical for agencies to investigate emerging technologies, develop a strategic plan to address future needs and transition their existing networks, hardware and software to technologies that will meet those needs for at least the next five years. In order to accomplish this it is necessary to have a basic understanding of what wireless technologies are available today and what technologies are emerging in the market place.

Commercial Public Wireless Networks

The first radiotelephone service was introduced in the United States at the end of the 1940s, and was meant to connect mobile users in cars to the public fixed network. In the 1960s, a new system launched by Bell Systems, called "Improved Mobile Telephone Service" (IMTS), brought many improvements like direct dialing and higher bandwidth.[v] Since the advent of the first radiotelephones, commercial public wireless networks have exploded worldwide driven by consumer demand. These networks have become fast and reliable with redundant systems most private wireless networks cannot match.

Commercial public wireless networks provide a number of advantages for law enforcement. They have proven to be very reliable, have wide area coverage, are fast networks compared with the private radio networks most law enforcement agencies have deployed, require minimal capital outlay for network set-up and do not require private radio frequency acquisition. These networks use privately held radio frequencies that are

protected from eavesdropping under state and federal telecommunications laws.

There are currently three generations of commercial public wireless networks operating. The third generation is an emerging technology. This technology is currently available in limited areas (most outside of the United States) and is being used by a limited number of consumers. It will likely take several years for third generation networks to be fully implemented.[vi]

First Generation - (1G)

The first analog cellular systems were developed in the late 1960s and early 1970s. Analog systems for mobile communications saw two key improvements during the 1970s: the invention of the microprocessor and the digitization of the control link between the mobile phone and the cell site.[vii] Many law enforcement agencies in the United States are currently using first generation networks.

Second Generation - (2G)

Digital cellular systems were first developed at the end of the 1980s. These systems digitized not only the control link but also the voice signal. The new system provided better quality and higher capacity at lower cost to consumers.[viii]

CDMA (Code Division Multiple Access), a spread spectrum technology, that transmits a simultaneous signal over a shared portion of the spectrum using a code division based system, which encodes multiple conversations. A Second Generation system operates most commonly in the 800 MHz and 1900 MHz band. Second Generation CDMA offers 8 to 10 times the capacity of analog systems. [ix]

TDMA (Time Division Multiple Access) a wireless technology that interweaves multiple digital signals onto a single high-speed channel using time division technology. TDMA divides each channel into three sub-channels providing service to three users instead of one. [x]

GSM (Global Systems for Mobile Communications) is a digital cellular phone technology based on TDMA technology. Predominantly a voice technology, GSM provides short messaging service that enables text messaging up to 160 characters in length at 9.6 Kbps transfer rate. [xi]

Evolution Path (2.5G)

GPRS (General Packet Radio Service) is an evolutionary enhancement to GSM technology that enables continuous flows of IP data packets at up to 170 Kbps. GPRS allows users to be continuously connected while only consuming network resources when sending or receiving, allowing users to enjoy tenfold price-performance improvements.[xii] GPRS functions on the GSM network which has 450 million subscribers and 392 networks using the standard. Over 135 wireless carriers are in various stages of GPRS deployment making GPRS the world's ubiquitous data network standard. [xiii]

EDGE (Enhanced Data rates for Global Evolution) is the next evolution of GPRS, that further enhances GSM and TDMA wireless systems by increasing data throughput to 384 Kbps (theoretical speed) while meeting essentially the same bandwidth occupancy of the original GPRS signal. EDGE is backward capable to GPRS allowing users to remain on the slower GPRS system if it meets their needs.[xiv] Edge service is emerging in large

United States markets. This service while approaching 3G standards is still considered a 2.5G service due to actual performance bandwidth and speed.

Third Generation – (3G)

Third Generation is defined by the International Telecommunication Union-2000 as networks which deliver improved system capacity and spectrum efficiency over the 2G systems and support data services at minimum transmission rates of 144 kbps in mobile (outdoor) and 2Mbps in fixed (indoor) environments.

CDMA 2000 (Code Division Multiple Access 2000), 1X is the IS-95 evolution to third generation technology. This technology can support wireless data speeds of up to 153Kbps, 10 times rates previously available on a single 1.25MHz carrier. CDMA 2000 is an efficient, robust technology supporting both voice and data. CDMA 2000 is backward capable to CDMA and is currently available in limited U.S. markets. There is some controversy over whether this service is 2.5G or 3G. CDMA 2000 1XEV-DO is a packet data system designed to enable operators to provide high speed data rates up to 2.4Mbps, up to three times the capacity of 1X. This service is not currently available in U.S. markets, however, it is the next step in the migration of CDMA technology.[xv]

WCDMA (Direct Spread Code Division Multiple Access) is the next step in the migration for GSM network providers. WCDMA has theoretical data speeds of 2Mbps. and will require new end user hardware.[xvi]

UMTS (Universal Mobile Telecommunications Systems), the European implementation of 3G wireless systems, provides service in the 2GHz band. UMTS is expected to provide high-speed data transfer while still allowing voice calls.[xvii]

IEEE 802.20

Institute of Electrical and Electronic Engineers 802.20 (IEEE) is the proposed WiFi answer to the 3G wireless wide area network market.[xviii] WiFi, short for wireless fidelity is the term generically used when referring to any type of 802.11 networks. This technology will be explained more fully on page 11. The term is a registered trademark of the WiFi Alliance This technology if approved and deployed would likely provide a true 3G wide area network that would easily interface with 802.11 local area networks and 802.16 metropolitan area networks.

Third Generation Summary

While third generation technologies will play a major role in meeting law enforcement's wireless needs over the next five years, the networks have some limitations. Commercial public wireless networks are consumer driven. While this creates the competition which drives advances in the technology, it means law enforcement will have minimal input into the architecture of the systems or the direction of the technology. Networks which customers are using today may be outdated and unsupported within a few years of their inception. Law enforcement competes for available bandwidth on the network with all other subscribers. Overusing networks can result in poor performance.

Third Generation networks have good authentification security to protect the networks from unauthorized use, but have minimal encryption security. These networks have gone to floating address systems in order to deal with the growing numbers of

subscribers with a limited number of available addresses. Many states including California still require fixed Internet Protocol (IP) addressing in order to transmit criminal records information. Many states including California require 128 bit encryption. A number of software and hardware vendors are now addressing these issues by providing middle-ware, which provides extra encryption and fixed IP addressing.

Fourth Generation – (4G)

The standards for the long-term future of commercial public wireless networks have not yet been established. Jon Fortt **,** in his article, Research Forum Leader Takes On Wireless Challenge, documents the ongoing fourth generation controversy. Implementation of 4G networks is estimated to be as many as 10 years off. According to Mikko Uusitalo, Chairman of the Wireless World Research Forum, when 4G does arrive; it could operate at 100 megabits a second, nearly 10 times faster than wireless hot spots (802.11). Uusitalo's goal is to have 4G be a world wide standard to avoid a repeat of the situation in the United States where there are three major incompatible cell phone networks, CDMA, GSM and IDEN, fighting for survival. In Europe, there is one: GSM. Michael Powell, chairman of the Federal Communications Commission, is among many in the United States that question the necessity of the united approach. He points out that while European countries all operate on the same type of GSM/GPRS network, their monolithic approach did not help them bring the faster 3G wireless networks into being any quicker. ``They destroyed 3G for themselves, for the most part," Powell said. He suggests future cell phone chips will enable phones to operate on any global network. ``If

your phone has a chip in it that can pick any spectrum, why do you care what they pick?" Uusitalo would like to see a blueprint for 4G worked out by 2007.[xix]

Ultra Wide Band (UWB)

In 2002, the Federal Communications Commission approved the commercial use of Ultra Wide Band (UWB) technology. Initially established as a military application, UWB is the newest wireless personal area network technology. A low cost and low power wireless technology, UWB uses a wide, flat signal that pulses rapidly. In addition to being able to transmit data at rates between 100 Mbps and 500 Mbps, these signals can pass through doors and other obstacles that tend to reflect signals at bandwidths that are more limited and at higher power levels. This allows the technology to be useful in detecting what is behind walls or buried underground. This technology is now being looked at by a number of commercial providers. It has potential to achieve speeds of 500 Mbps at a much lower cost than 802.11 networks. UWB signals are so powerful that they could cause interference to other wireless operations.[xx]

OFDM (Orthogonal Frequency Division Multiplexing)

Orthogonal Frequency Division Multiplexing (OFDM) is one of the most notable technologies moving towards the post 3G environment. The technology selected by the IEEE for 802.11a standard could eventually lead to chips that will allow for multi-carrier access. The main limitation of this technology is range (see WiFi Networks on page 12 for more information).[xxi]

Private Data Networks

Private Data Radio

Legacy private radio data systems are in common usage by law enforcement for data transmission. These systems commonly share bandwidth between voice and data making them slow, with insufficient bandwidth to handle emerging wireless applications. The modernization of private data systems faces two major hurdles, the cost of building networks and the availability of additional spectrum within dedicated bandwidth.

In 1997, Congress, responding to the recent focus on interoperability and Homeland Security, recognized public safety's need for spectrum and reallocated 24 MHz of spectrum from television channels in the 746 – 806 MHz band. This band is commonly referred to as the 700 MHz band. The 700 MHz band's close proximity to public safety's current 800 MHz can allow agencies to expand their current 800 MHz narrowband voice and data systems and implement advanced wide area high speed data networks.[xxii] Unfortunately, in order for public agencies to use the reallocated spectrum, any TV stations currently operating in the spectrum must have ceased operations. This is as many as seven channels in any given market.[xxiii] Currently an estimated 54% of the country's population lives in areas where public safety has no access to the 700 spectrum. An additional 16% of the population lives in areas where public safety has access to only half of the 700 MHz spectrum.[xxiv]

WiFi Networks

IEEE 802.11 is a type of radio technology used for wireless local area networks. The standard has been developed by the IEEE (Institute of Electrical and Electronic

Engineers). The IEEE is an organization which develops standards for electronic and electrical technologies. The IEEE uses a series of numbers similar to the Decimal system used in libraries to differentiate between the various technologies t categorizes.[xxv] WiFi, short for wireless fidelity is the term generically used when referring to any type of 802.11 networks. The term is a registered trademark of the WiFi Alliance.[xxvi] The WiFi alliance is a non-profit organization formed in 1999 for certifying the interoperability of IEEE 802.11 products and to promote WiFi as the wireless LAN (Local Area Network) standard.[xxvii]

There are several benefits to WiFi networks: they increase mobility; provide significant bandwidth increases over current wireless networks; are compatible with networks using Internet Protocol; do not require private radio frequency acquisition; and the capital outlay for network set-up is moderate.

There are three 802.11 standards operating in the United States on different radio frequencies. The first standard is for wireless LANs operating in the 2.4 GHZ spectrum (802.11b) with an 11 Mbps bandwidth. The second standard is for wireless LANs operating in the 5 GHz frequency with a 54 Mbs bandwidth (802.11a). The third standard is operating at the 2.4 Ghz spectrum with a 54 Mbs bandwidth (802.11g). [xxviii]

Current WiFi networks have a number of inherent limitations for public safety use. The frequencies used are in the public spectrum and have limited availability. This means that local businesses, government agencies and even individual households are setting up networks and transmitting within this narrow spectrum. This has created interference issues and security issues for these networks. Public safety must have networks that have network access (authentication) and data protection (encryption).

Original 802.11 networks had a security protocol that had limited security standards that have proven to be easily defeated.[xxix] The IEEE is currently working on developing a new standard for WLAN security, 802.11i. This specification will upgrade the current authentication standards and encryption made available in mid 2003. [xxx] These new security advances, along with other network security measures such as Virtual Private Networks (VPN), can make WiFi networks secure enough for public safety use.

The limited range, 300 feet from the hub for 802.11b, makes building municipal area networks with adequate coverage difficult. Even with the combination of wireless-to-wireless (Ad-Hoc) networks and wireless to wire (Infrastructure) networks and wireless node to node (mesh) networks, it would be difficult and likely expensive for a city to provide full coverage within their jurisdiction with a WiFi network.[xxxi]

WirelessMAN

Institute of Electrical and Electronic Engineers 802.16 standard, known as WiMAX, may have the greatest potential for law enforcement in the 802 standard technology. This emerging technology is known as WirelessMAN air interface or Air Interface for Fixed Broadband Wireless Access Systems. The principle advantage of this standard is a cell radius of up to 30 miles, typically averaging 4-6 miles, non-line of sight performance. This technology can provide a metropolitan area network backbone to 802.11 local area networks. With data rates up to 75 Mbps and bandwidth of 20 MHz , 802.16 networks can provide services at the broadband landline level. This technology is capable of handling both streaming video and voice over IP.[xxxii]

Satellite Data Networks

The proliferation of satellite television services has provided the backbone for commercial satellite data networks. These networks have download speeds of 400 to 1500 Kbps and upload speeds between 30 to 60 Kbps. These systems are excellent for downloading data to fixed locations and are available throughout the United States. They currently have limited upload speeds and require directional dish antennas.[xxxiii] The current limitation of directional dish antennas and the current cost of data transmission make these networks impractical for law enforcement at this time. The technology should be watched for future consideration. The federal government has significant investment in satellite data technology that is not currently available to local law enforcement. If these technologies were made available at some time in the future, the networks could have significant impact on interoperability.

Future Applications

In addition to identifying emerging and future wireless technologies, it is critical for law enforcement managers to have a good understanding of the type of applications law enforcement is likely to be using in the future. It is likely law enforcement will continue to use most of its current field applications. There are three main categories of future applications worth taking a closer look at, streaming video, Internet Protocol (IP) based applications and applications for personal data devices.

Streaming Video

Law enforcement has long seen the value of remotely accessing video for surveillance, officer safety and liability management. Most agencies have experience with remote video using wired networks or video storage devices. High speed wireless networks can provide law enforcement with the ability to monitor remote sites from mobile positions, monitor mobile to mobile or monitor mobile activity from fixed sites.[xxxiv]

The technology for monitoring remote streaming video over wireless IP devices currently exists today. The limiting factor for wireless access to remote video has been the speed and bandwidth of the wireless networks being used by law enforcement. Current wireless networks capable of 9.6 baud or 19.2 kbs are not capable of video transmission or reception. Emerging networks, such a GPRS and CDMA, are capable of sending and receiving short video clips and video frames but cannot handle live streaming video. The Edge upgrade to the GPRS network has advertised speeds capable of handling live streaming video, however this is realistic only when optimal network conditions exist. True third generation networks, such as CDMA2000 and WCDMA, will bring public wide area networks (WAN) into the streaming video business within the next five years.

WiFi, while not in common use by law enforcement, is capable of handling streaming video applications.[xxxv] While coverage, cost of implementation and security issues limit WiFi as total wireless solution for law enforcement, network bandwidth and speed make WiFi a good solution for streaming video applications. Emerging WiMax technology promises to resolve some of these issues and will likely be the best technology available for streaming video applications in the next five years.

Internet Protocol Based Applications

A study by the Universal Mobile Telecommunications Systems (UMTS) Forum found that mobile intranet/extranet access and customized infotainment would become the dominant wireless data services in the next 5 to 10 years.[xxxvi] Internet Protocol, Intranets, Virtual Private Networks and server based terminal emulation software has provided law enforcement with the infrastructure that will allow mobile access to traditional office applications and databases. Internet Protocol based applications will facilitate the sharing of databases between government agencies allowing the mobile user real-time access to databases traditionally only available over landline connections.

Videophone technology will permit person to person or person to multiparty, real-time video, plus voice. This technology could be used for conducting briefings in the field, training and provide more personal contact between field officers and clients than traditional phone calls or text messaging.[xxxvii] Internet Protocol voice is a conversational voice service that can transmit to and from all types of networks. This technology would allow data devices to also act as a private radio system. This technology has the potential of replacing traditional police radio systems or providing a backup to them.

Interactive customer care applications will provide the ability for systems managers to remotely scan mobile units and reset terminal settings, upgrade software and install software while the mobile unit remains in the field. Multimedia services applications will allow user terminals to address, access and present different types of multimedia objects. These applications will be used for in field training and public presentations.

Voice Portal applications provide the ability to access information and conduct transactions with voice commands. This technology will soon become accurate enough for use in the mobile environment. Voice portal applications will allow for safer and more efficient use of mobile applications.[xxxviii]

Personal Data Device Applications

Personal Data Device hardware and software applications, as they have in the general market place, will likely have significant impact on the future of wireless in the law enforcement community. [xxxix] Advances in wireless data transmission are energizing the vision of making the untethered use of Internet/intranet devices a reality.[xl] While law enforcement has been a leader in connecting its mobile work force, it has generally been tied to the patrol car. In the future, law enforcement officers will likely access information from a number of handheld or wearable devices. This includes wearable, heads-up displays that allow emulation of the car's mobile computer, personal video devices that are capable of transmitting and storing video and audio from an officer's person and personal data devices capable of entering reports, records information and creating citations.[xli]

Summary

In order for law enforcement to meet its wireless needs over the next five years, its migration path should include networks capable of servicing applications requiring robust wide area wireless networks such as third generation commercial networks, metropolitan area networks such as WirelessMAN and personal area networks such as

UWB. Wide area networks provide the coverage necessary for agencies to function regionally. Metropolitan area networks provide the ability to transmit large volumes of data, video and voice at high speeds without accumulating high usage fees. Personal area networks provide the vital link between personal computing devices and wide area or metropolitan area networks.

This chapter has examined existing, emerging and future wireless technologies. Now it is necessary to look at future trends and events that could impact law enforcement's ability to use those technologies to meet future wireless data transmission needs in a mid-size urban law enforcement agency by 2009. These trends and events and their impact on the issue statement will be examined in the following chapter.

Chapter II

Futures Study

Nominal Group Technique

Process

In January, 2003, a Nominal Group Technique session was held to help identify trends and events that will impact the way emerging wireless technologies will be used by a mid-sized urban law enforcement agency to address wireless data transmission needs by 2009.

The Nominal Group Technique is a structured process designed to provide equal input and limit dominant participants. This group was tasked with identifying trends and events that will impact the issue statement then quantified their opinions using an established rating process.

The process used a group of knowledgeable, diverse panel members to identify and evaluate the impact of future trends and events on the issue statement**.** The results of this exercise should identify those trends and events that should be encouraged or discouraged in order to benefit the ability of law enforcement to use emerging wireless technology to meet its data needs by 2009.

The panel consisted of eight members: two representing public safety, two representing municipal information systems departments, three representing wireless technology vendors and one computer programmer. The panel members and their representative organizations are listed in Appendix I.

Trend Analysis

Trends are a series of incidents or events taking place, which seem to indicate a direction in which a particular issue may be heading. It is based on the past, present and future and can be quantitative or qualitative. Each panel member was asked to name trends that they felt are occurring that will have an impact, positive or negative, on the future of this technology for use by law enforcement. The NGT panel developed a list of the trends (Appendix II) that each panel member offered for discussion, then pared down this list to nine major trends that the group felt would have the most impact on the issue statement.

For each of the nine trends, the group members were asked to quantify the increase or decrease of the trends five years ago, five years from today and ten years from today in relation to today. They also rated the level of concern regarding the trends impact on the issue statement using a scale of 1, little concern to 10, great concern. The statistical median of the individual results represents the group's final product. The results of this discussion are summarized in Table 2-1.

Table 2-1 Trend Summary

Trend	-5 Years	Today	+5 Years	+10 Years	Concern (1-10)
T-1 Bandwidth availability in the wireless marketplace	50	100	1000	2000	7
T-2 Availability of funding for technology projects	100	100	100	100	8
T-3 Level of Interoperability between government agencies	75	100	300	500	7
T-4 Number of wireless technology applications available to law enforcement	25	100	300	450	8
T-5 Number of vendors offering consolidated wireless services.	50	100	150	175	2
T-6 Availability of wireless network coverage	80	100	200	400	8.5
T-7 Level of data security	75	100	150	200	8
T-8 The cost of maintaining and managing technology	80	100	100	150	8
T-9 Amount of technological knowledge of employment pool	50	100	200	250	5

Trend 1: Bandwidth availability in the wireless marketplace

The panel felt that the general market for wireless technology along with competition in the industry would drive the industry to increase the wireless bandwidth availability ten fold in the next five years and even more in the next ten years. The panel cited the emergence of third generation wireless, 802.11 and the anticipation of fourth generation technology within five to ten years. One panelist suggested that the availability of bandwidth would flatten out between five and ten years due to the limitations of wireless technologies and lack of demand. The panel felt law enforcement was not a significant driving factor in the trend of increasing bandwidth, although they felt law enforcement had been a significant factor in getting the business community to understand the advantages of mobile computing. The panel was concerned about the availability of bandwidth in the general market place and felt it would be significant for law enforcement to address wireless data transmission needs.

Trend 2: Availability of funding for technology projects

This group of NGT panelists were mixed on the outlook for technology funding availability. As a result of the statistical median, the panel found that funding for technology projects would remain relatively constant over the next ten years. Some in the group felt there would be a trend for modest increases, while others felt there would be modest decreases or that the trend would be flat. In general, the panel felt this trend was impacted by economic cycles and the availability of federal and state grant funding. One of the panelists felt the spending would increase over the next five years and then decrease after the cost of infrastructure building was complete. All of the panel

expressed a high level of concern regarding this trend, as the availability of funding would significantly impact law enforcement's ability to take advantage of emerging technologies.

Trend 3: Level of interoperability between government agencies

The panel defined this trend as the degree to which government agencies have the technological capability and actually do share databases. The panel felt that since the September 11th attacks, there has been an increased emphasis on interoperability at all levels and that this emphasis would result in increased capability. One panelist pointed out that we currently have technology to handle the needs but that cultural changes take longer than technological changes. The entire panel agreed that this would be an increasing trend, tripling over the next five to ten years. The panel felt this trend would have significant impact on the issue statement because it will likely be important to have access to these new shared databases in the field. The panel felt that the drive for interoperability could create funding opportunities, availability of spectrum and encourage legislation of public networks. One of the panelist felt that while this trend was likely to increase, it was not relevant to wireless technology. This panelist felt that agencies' existing networks would handle this type of need and it would not impact how we will use emerging technology.

Trend 4: The number of wireless technology applications available to law enforcement

The panel defined this trend as the availability of software applications that are designed to be used in a wireless environment and applicable to law enforcements needs.

The panel believed the number of wireless technology applications available will increase significantly over the next ten years. One of the panelists commented that there will be applications developed over the next ten years that we cannot even imagine today. One panelist felt there might be a reduction in software applications after 5 years due to the development of hardware, that will not require software applications. The panel was concerned that the number of applications available will influence the wireless transmission bandwidth needs, what we use wireless for, and, therefore, how law enforcement will use emerging technologies.

Trend 5: Number of vendors offering consolidated wireless services

The panel defined this trend as the number of vendors in the market place providing voice, data and digital video capable wireless service. The panel felt there would be a moderate increase in the number of available vendors over the next five and ten years. The panel felt that the commercial market vendors would likely not have significant numbers of new entries into the marketplace due to stiff competition, consolidation and lack of available spectrum. The panel did see a trend towards increased numbers of government enterprise vendors and small business local area providers. Overall, the panel was not particularly concerned with this trend's impact on the issue statement. Two panelists disagreed and felt the availability of vendors would have at least moderate impact on the cost of available services and therefore impact the ability to take advantage of emerging technologies.

Trend 6:Availability of wireless network coverage

The panel defined this trend as the geographical availability of wireless network coverage. The panel saw this trend as including improved coverage in existing service areas (signal strength) and the buildout of networks in areas not currently covered (availability) by wireless networks.

The panel found this trend to have been steadily increasing and felt it would continue to have a steady increase over the next five and ten years. One of the panelists noted that the proliferation of networks has been slowed by lower than expected demand, increased costs and government regulations of transmuting towers. One panelist pointed out that most major markets have good coverage currently and that it will be difficult for providers to justify buildout in markets that do not have the return necessary to pay for the capital outlay required to build. The panel was very concerned that this trend would have significant impact on how law enforcement will use emerging wireless technologies. The panel felt availability, signal strength and commercial network coverage would have significant influence on what type of technology law enforcement agencies choose to use over the next five years.

Trend 7: Level of data security

The panel defined this trend as the degree of data security provided within wireless networks. The panel felt wireless networks are more secure today than they were five years ago, pointing out better encryption, firewalls, and VPN technology. One panelist had a dissenting view, feeling that networks were more secure five years ago because they had fewer external connections. The panel felt that overall security of

wireless networks would steadily increase over the next five and ten years due to client demand. One member of the panel felt that vendors may begin providing secure and unsecured services, providing higher speed service for those clients who do not need the security measures that tend to slow network speeds. The panel was concerned about this trend and felt it would be a significant issue to law enforcement because of the type of applications being deployed and the type of data being transmitted.

Trend 8: The cost of maintaining and managing technology

The panel defined this trend as how much it costs to maintain technologies associated with wireless networks and included the cost of managing these technologies. This panel felt that there has been a moderate cost increase in maintaining and managing technology over the past five years. The panel felt that this cost would flatten out over the next five years and have a moderate increase between five years and ten years in the future. The panel felt that there is currently significant pressure from clients for maintenance costs to be included in initial purchase or within the standard service fee. The panelists pointed out that many systems are self-diagnosing and that this will continue to be a trend in the future. The panelists felt that at some point these costs would have to begin increasing again, due simply to the amount of technology being deployed. They expressed significant concern that this trend would impact the issue statement. They commented that maintenance cost, degree of difficulty and time consumption would all be factors in considering what type of technology to use.

Trend 9: Amount of technological knowledge of employment pool

The panel defined this trend as the degree of technical knowledge of employees, both current and future. The panel felt the technical knowledge level of employees has doubled in the past five years and will double again over the next five years. They see the knowledge level continuing to increase between five and ten years out but at a slower rate. The panel felt the trend would slow due to technology booms creating knowledge overload and the limited ability of people to absorb this information. The panel had moderate concern about this trend. The general opinion was that it would be necessary for employees to have at least minimal technological knowledge in order for law enforcement to take advantage of emerging wireless technologies.

Event Analysis

Events are different from trends in that events are singular occurrences. Future events occur at a specific time and date and have not yet occurred. Each panel member was asked to identify future events that they felt will or may occur that would have a significant impact, positive or negative, on the future of law enforcement's use of wireless technology. The NGT panel developed a list of the events (see Appendix III) that each panel member offered for discussion, then pared down this list to 8 major events that the group felt would have the most impact on the issue statement. The panel identified the first year they felt the identified event could take place and then the likelihood it would take place within five years and within ten years. Finally, the panel quantified the impact of the event on the issue statement using a scale of +10 (positive impact) to –10 (negative impact). The statistical median of the individual results

represents the group's final product. The results of this discussion are summarized in Table 2-2.

Event 1: 100 mb wireless network deployed

The panel felt there was only a 50% chance that 100 mb technology would be developed and deployed in the next five years but was certain it would happen in the next ten years. The panel felt this would be a very significant positive event, as it would meet foreseeable application needs for the next ten years.

Event 2: Hacker infiltration of national criminal justice information database becomes public

After some discussion, the panel commented that this event was likely to occur within the next 10 years and may have already taken place; however, if so, it has been kept quiet. A public exposure of such an event would likely create increased security rules that would make access to wireless technology more difficult and more expensive for law enforcement. One panelist felt the event would have a significant positive impact as funding to provide more secure networks would be made available allowing law enforcement to upgrade their networks and take advantage of new and emerging technologies. Two panelists felt the event would have no impact as people have become accustom to hacker incidents and would pay little attention to the event. Some members of the panel felt this event would have significant negative impact if the infiltration were made public. As a result of diverse opinions and applying the statistical median, the group's final rating for this event appears to be an insignificant negative impact.

Table 2-2 Event Summary

Event	**Year > 0**	**+5 Years**	**+10 Years**	**Impact** **(-10 to + 10)**
E-1 100 mb wireless network deployed	5	50	100	+8
E-2 Hacker infiltrates national criminal justice information database	5	30	50	-1
E-3 Police sued after using wireless surveillance	3	90	100	0
E-4 Scientists prove EMI causes brain cancer	10	0	8	-5
E-5 DOJ approves use of Internet for CORI.	2	100	100	+5
E-6 FCC re-allocates spectrum to public safety	5	75	100	+5
E-7 FCC requires wireless carriers to provide public safety priority access.	5	25	50	+3
E-8 Feds fund interoperability at national level.	3	25	50	+8

Event 3: Police sued after using wireless surveillance

The panel defined this event as a high profile lawsuit. They felt this event could occur in three years, has a high probability of occurring in five and a certainty of occurring within ten. The panel was split on what impact the event would have on the issue statement. Some of the panelists felt that this event would have a negative impact if the lawsuit was successful. The majority of the panel felt the event would have no impact and one panelist felt the event would have a positive impact as this panelist felt the lawsuit would be unsuccessful.

Event 4: Scientists prove Electrical Magnetic Interference (EMI) causes brain cancer

The panel felt that this event was very unlikely to occur within the next ten years and could not see it occurring for at least ten years. The group had a mixed opinion regarding the impact this event would have. About half the group felt the event would have a significant negative impact while half the group felt the impact would be slightly negative or neutral. The group that felt the impact would be minimal felt that the use of wireless devices would be so prevalent in society that we would be too dependent on the technology to change our use habits.

Event 5: DOJ approves use of Internet for criminal offender records information (CORI)

The panel felt this event would take place within 5 years. The panel felt this event would have a positive impact by providing law enforcement with access to many emerging applications and technologies developed with browser technology and by providing access to less expensive technologies designed for the mass market. Two

members felt the impact would have no significance as most of these applications and technologies can be accessed from private IP networks. One member pointed out that the federal government was already using the Internet to transmit criminal justice information. Overall, the consensus was that that use of the Internet for CORI would positively impact law enforcement's ability to use emerging wireless technologies.

Event 6: FCC re-allocates spectrum to public safety

The panel defined this event as the Federal Communications Commission assigning private radio spectrum to law enforcement agencies for use in developing wireless data networks. The panel felt the first year this could occur was five years out. They felt there was a good likelihood this would occur in five years and were sure it would occur within ten. The panel saw pressure from law enforcement on the federal government as the driving factor. Overall, the panel believed this would have a positive impact on law enforcement's ability to use emerging wireless technologies.

Event 7: FCC requires wireless carriers to provide public safety priority access

The panel felt this event could take place in five years. The panelists felt there was some chance of this occurring within five years and a 50% chance within ten years. They were mixed on their opinion of the impact of this event. Interestingly, the commercial providers on the panel felt this would have a significant positive impact; the public agency members on the panel thought the impact would be positive but not as significant as their commercial counterparts. The commercial vendor representatives commented that they are continually asked to include network access and prioritization

clauses in their contracts with government entities. A split in opinions on this event resulted in an overall low, positive impact rating.

Event 8: Feds fund interoperability at national level

The definition of interoperability for the purpose of this event is the ability to communicate by voice and data between agencies. The panel felt that while this would be difficult and expensive there was a fair chance interoperability could be funded through Homeland Security funds in the next ten years. If this were to occur, the panel felt that the funding would have a significant positive impact on law enforcements access to wireless technology and their ability to upgrade to emerging technologies

Cross Impact Analysis

After identifying the trends and events that could most impact the issue, the panel was asked to consider the following questions: "If an event occurs, what effect will it have on a particular trend? Will that impact have a positive or negative effect on the particular trend?" The cross impact analysis identifies the positive or negative impact using a scale of +5 (positive impact) to –5 (negative impact). The statistical median of the individual results represents the group's final product. The results of this discussion are summarized in Table 2-3.

Table 2-3 Cross Impact Table –5 (negative impact) to +5 (positive impact)

	T1	**T2**	**T3**	**T4**	**T5**	**T6**	**T7**	**T8**	**T9**
E1	+5	0	+2	+3	0	+3	0	0	0
E2	0	0	-3	0	0	0	+4	-1	0
E3	0	-2	0	0	0	0	0	0	0
E4	0	-3	0	-4	-2	-3	0	-3	0
E5	0	0	+3	+3	0	0	-2	+2	0
E6	+3	+2	+3	+2	0	+2	+3	0	0
E7	0	0	+2	0	0	+4	+1	+3	0
E8	0	+2	+3	+3	0	+3	+3	-1	0

The panel found that event 1 “100 mb wireless network deployed” would have a positive or null impact on all of the trends. While the panel found this event to be important to law enforcement, it is impacted by events taking place in the much larger general market place.

Events 2, “hacker infiltrates national criminal justice information database,” and 4, “Scientists prove EMI cases brain cancer” have a negative or null impact on all of the trends except trend 7, “level of data security,” which they felt would increase after a publicized hacking event. The panel felt it would be in law enforcement’s best interest to maintain a high security level on its networks in order to avoid event 2. While the panel felt that event 4 was very unlikely, they felt this event would have significant negative impact on the entire wireless market including public safety.

The panel suggested that event 5, “DOJ approves use of Internet for criminal records information” would positively or null impact all of the trends except trend 7, “The level of data security.” They felt there would be an acceptable amount of security loss that could be mitigated by security protocols. The panel felt this event should be encouraged by public safety managers.

Event 6, “FCC reallocates spectrum to public safety” and event 7, “FCC requires wireless carriers to provide public safety priority access” were found to positively or null impact all of the trends and while it would not advantage the general marketplace, they are events the panel felt would likely occur in the next 5 years.

Not surprisingly, trend 2 “Availability of funding for technology projects” is positively impacted by the events that provided federal funding or allocation of spectrum. The panel felt that it is likely that some type of funding would be made available by the federal government at some point in the next 5 to 10 years and that it would be beneficial for law enforcement to encourage these types of events.

Alternative Future Scenarios

In this section three scenarios will be used to illustrate possible alternative futures. Each scenario will depict a possible future based on the decisions agencies make in the area of wireless technology and how trends and future events may impact those decisions. The purpose of this exercise is to help agencies identify the best strategy and those events and trends that can help or hinder their implementation. The three scenarios describe a worst case, normative and best case scenario focusing on law enforcement’s future use of wireless technologies.

Scenario 1

Worst Case

Norcal January 4, 2009

It was a cold morning as Officer Zenon Dragan began his patrol car checkout procedures. Zenon sat in the driver's seat and stared at the integrated computer display in the dash. He thought to himself, what a waste. It was less than six months prior that the 14-year-old computer hacker had broken into the new homeland security integrated database through the old CDPD wireless network. That, in itself, would not have been so bad, he thought. But no, this hacker had to spam email the data bases to every Internet user on the western Internet grid. He remembered it was just under a year ago that some quack doctor announced that EMI caused brain cancer so the department decided not to move forward with their plans to upgrade their wireless networks. This was just not a good year for technology.

As Zenon drove out the back lot, he remembered that he had to tell the dispatcher via radio that he was in service. Zenon, a seven year veteran, had never had to use the radio to put himself in service. He thought to himself that it sure hadn't taken long for the feds to take the knee jerk reaction of shutting down the old CDPD wireless network. He was angry that his department had not upgraded their wireless networks three years ago when their CDPD vendor quit supporting the technology and sold the network. The company that took over the network lacked the resources or the desire to upgrade the network's security. Zenon said aloud "I guess it's no big deal, the network did not work half the time anyway".

Zenon drove to his beat and began patrolling the East area of his district where the city was experiencing a series of auto thefts. While patrolling in the business park, he decided to stop a car with a missing front plate. Zenon remembers that he has to call the plate number in on the radio. However, he forgets to provide his location and is sternly reminded by the dispatcher. Zenon thinks to himself, what a waste of time. For as long as Zenon could remember, his patrol car location was reported directly to dispatch over the wireless network using GPS technology. Now that their wireless network was disabled, not even the most simple and critical safety technology was working. He thought the union should do something about this. Just after getting the driver's license, Zenon heard robbery tone broadcast followed by a bank robbery alarm dispatch. He knew that he should not try to run the license on the radio while the robbery alarm call was in progress. He was frustrated and wrote the driver a citation for the front plate violation and not having his registration card in the vehicle. It felt strange to write the citation on paper as he had been using an electronic integrated citation program for three years. This, too, was part of the department's wireless network. Another piece of useless technology, he thought. It wasn't until 15 minutes later that the dispatcher advised Zenon that the license plate was stolen. When he finally ran the driver, he found out that he was a parolee at large. Zenon thought in disgust, a great start to the day, and wondered how many such days would follow.

Senario 2

Normative

Norcal, January 4, 2009

Officer Zenon Dragan began his daily routine by checking out his patrol car. A cold morning, even for January, he thought as he wondered if the cold would affect his computer display panel integrated into the dash of his patrol car. “Computer email display,” he commanded. Less than a second later Zenon’s email displayed on the screen. After viewing a couple of junk emails (that’s what Zenon refers to all personnel email as), he commands, “check voice mail.” A second later, “VAR.,” voice activated response, answers, “You have no new messages.” Zenon looks over to his trainee sitting in the passenger seat and tells her, “You should have been around in the good old days of computers. Before the department installed our multimodal high speed network, it took forever to get anything and you had to go to the station to get your email.” This was Officer Janis Sales’ second day in the field-training program. As the officers pulled out of the parking lot, VAR announced that there are two incoming BOLOS. Janis and Zenon look at the pictures of two people wanted by their narcotics detectives. Zenon recognizes one of them but can’t remember why. He commands, “check in house records.” Sure enough, Zenon had arrested the guy last year. Zenon commands “get report.” The report instantly appears on the screen and Zenon begins to read through it. Zenon finds a notation about a girlfriend’s house and decides he will check it later. He thinks to himself, how did we ever get along without high-speed wireless access?

As they pull onto Main Street, Officer Dragon decides to stop a car for rolling through a stop sign. Great training opportunity, he thinks. He turns to Janis and tells her

“put us out on a stop.” Janis commands, “computer - traffic stop – 1Mary Mary Frank 224.” VAR responds, “ John 11, traffic stop, 115 Main Street, 1Mary Mary Frank 224,” a second later VAR reads and displays the wants and warrants and the registration information. Janis makes contact with the driver who tells her he lost his driver’s license. Zenon suggests to Janis that she check Cal ID. He explains to her that the Cal ID system is just one of many new Internet based databases they now have access to as a result of DOJ approving the use of the Internet two years ago. Janis runs the name the driver provided and finds the DMV photo does not match. Janis arrests the driver for providing false information and scans his thumbprint. Less than a minute later, they have the driver’s true identity and know he is wanted in Nevada.

After lunch, Zenon parked the patrol car under a tree and turned to Janis. He wanted to critique the DUI arrest she had made yesterday. Zenon commanded, “computer – access digital video – John 11 – January 3, 2009 – 1325 hours.” About 5 seconds later, a video clip appeared on Zenon’s screen. He reviewed the video with Janis. He thought to himself, what a great training tool being able to access the department’s car video database on demand from the patrol car.

Scenario 3

Best Case

Norcal, January 4, 2009

Ryan Lane, the Norcal City Information Systems technician, goes through his morning routine at the police department. He checks the National Homeland Security Information Network (NHSIN) server; a year after installation and all the bugs seemed to be worked out. Ryan remembers the fight between Homeland Security and the military over law enforcement's use of the military's worldwide high-speed wireless data network. He was glad that law enforcement won. He marveled at the innovative technology. Ryan moved on to the NHSIN Browser server and did his weekly usage backup. Another piece of Microsoft brilliance, he thought. Microsoft's new browser converter software allowed the feds to convert data from any database to a browser-based format allowing any law enforcement agency on the NHSIN to search any other database. It was brilliant, a national database at a fraction of the cost of building one from scratch. Ryan sat in front of the servers and watched the day watch officers begin to sign on.

Officer Paul Dorn liked to walk the sports park every morning at the beginning of his shift. Paul adjusted his headset and commanded, "Computer, briefing notes." Almost instantly, Sgt. Lance's face appeared on Paul's heads-up display. Paul watched the five-minute briefing then accessed his voice mail and email. He finished the half-mile walk and got back into his car. He loved the high-speed wireless network. He remembered how useful it was last month when he worked with a Reno, Nevada, officer on a child abduction case. He still car-to-car text messages with the officer once or twice a week. As Paul left the park, he was hailed by a motorist who complained of a long

back up on First Street. Paul accesses the city's Traffic Video System and views the three intersections along First Street. No collisions, just commute back up. Paul logs onto the high school parking lot cameras. The School Resource Officer had been complaining of kids smoking in the parking lot. Paul checked the three parking lot cameras and did not see anyone.

Paul decided to walk downtown; the merchants always liked to see him in the mornings. As Paul walked past the alleyway adjacent to the All Fall Down Bar, he saw a group of men standing in the shadows. Paul thought he recognized one of the men as a local drug dealer. Paul commanded, "Computer – records check – Dean Stanley." Paul's heads up display showed three possible. Paul commanded, "Computer – select number three – display photograph." Paul was right, and along with the photograph was a warrant hit out of Oregon. Paul completed Stanley's booking in his patrol car and transmitted it to the jail. Paul dropped his prisoner off at the drive-through drop and was out in just a couple of minutes. Paul could still remember the days of standing in line for up to an hour to book prisoners. As Paul pulled out of the drop off lane, he received a tone and then a National Terror Alert. Photographs of three men and a warning about threats to blow up a major bridge appeared on his display. Paul looked at the information and then commanded, "computer – save as patrol notes," he might want to review it again later. "Not a bad morning," he thought as he commanded his computer to show him off at the local coffee shop on a break.

Planning for the Future

The decisions being made by law enforcement today will have significant impact on the future of law enforcement's use of wireless technology. Law enforcement can choose to recognize trends and events that will impact the future and plan for a normative or best case future, or simply allow the future to happen and manage crisis. The next chapter will look at a sample strategic plan for wireless technology using a mid-size urban law enforcement agency as an example.

CHAPTER III

STRATEGIC PLANNING

Introduction

Wireless communications technology continues to experience tremendous growth in speed, bandwidth and quality of transmission. The next five years are likely to see technological improvements that will increase speeds and bandwidth 100 times over the technologies in general use today. The availability of these new wireless technologies will drive the development of wireless software and hardware in the public safety arena. These changes can have a significant positive impact on the work processes of mid-size urban law enforcement agencies like the Pleasanton Police Department. Successful law enforcement organizations must have the ability to think strategically, learn, anticipate change, adapt and act in order to take advantage of these emerging technologies. It is necessary to take a structured approach to planning in order to bring anticipation of the future to bear on decisions we make today.[xlii] This chapter will outline a strategic plan for the implementation and upgrade of wireless technology over a five year period. The Pleasanton Police Department will be used an example.

Organizational Description

The City of Pleasanton is a general law city operating with a City Council/City Manager form of government. As a general law city, Pleasanton's council structure, planning procedure and many other aspects of local government are controlled by state law. The Pleasanton city government provides a full range of services including those

related to police and fire protection, planning and building review, road construction and maintenance, water and sewer distribution and maintains a wide range of recreational/social services through its Parks and Community Services Department. The city, located approximately 60 miles east of San Francisco, California, has a population of 65,000 and covers an area of approximately 20 square miles.

The Pleasanton Police Department has 120 employees, including 84 sworn personnel and 10 managers. The Department has a chief of police as executive manager. The Chief of Police reports directly to the City Manager. The Department is divided into two divisions, Operations and Support Services, each managed by a police captain. Approximately 85% of all personnel function full or part-time in the field.

The Pleasanton Police Department has approximately 30 vehicles that are currently equipped with mobile data computers using a commercial cell data package delivery (CDPD) wireless network to transmit data. Current applications include access to records management systems, computer-aided dispatch, in-vehicle mapping, automated vehicle location system and field reporting. The department has a desire to develop a strategic plan designed to upgrade its current wireless technology to meet it data needs for the next five years.

Vision

In order to develop a strategic plan for an issue, in this case, how emerging and future wireless technologies will be used to meet needs by 2009, it is necessary for the organization to have a vision. The following is a proposed vision for the Pleasanton Police Department:

> The Pleasanton Police Department values the use of emerging wireless technologies to provide its mobile field work force untethered access to information in order to improve the efficiency, effectiveness and quality of services provided to our clients and the safety of employees.

In order to accomplish this vision, the Pleasanton Police Department will develop a specific strategic plan for the adoption and implementation of new wireless technology as part of its general strategic plan.

Goals

This strategic plan will address two goals, one involving the implementation of wireless network technologies and the other implementing wireless application technologies.

Goal #1 – Wireless Network Implementation

The Pleasanton Police Department will implement wireless network technology that will meet its wireless application needs for wide area networks, metropolitan area networks and personal area network applications.

Goal #2 – Wireless Application Implementation

The Pleasanton Police Department will implement leading edge wireless application technology that will provide field personnel with the tools to provide the community with more effective, efficient and safer policing services.

Organizational Analysis

In order to develop a strategic plan, it is important to analyze the internal strengths and weaknesses of an organization as well as the external opportunities and threats as they relate to the identified goals. This type of analysis provides an assessment of the organization's ability and willingness to accept and adopt change. This analysis is generally referred to as SWOT model.

Internal Weaknesses

Information technologies inside of the department are managed by the city Information Services Department. Police management does not have direct supervision or management of Information Services staff working in the police department. Role definition in the management and development of technology projects has been unclear and has resulted in implementation delays. The information systems technology knowledge base within the department is limited to a few key people. Mobile application technology knowledge is limited to one person. The loss of key personnel is likely to result in operational failures. Strategic planning in the area of wireless technology has been lacking in the past.

External Opportunities

The police department has historically received adequate support from city information systems staff. The Information Systems Department management has traditionally supported new wireless technology development and implementation in the police department.

City budgeting practices provide for a three-year replacement cycle for mobile computing equipment. This funding cycle provides the opportunity to update to meet changing network and application needs. AT&T's phase-out of CDPD wireless service has provided the catalyst to upgrade the department's wireless network.

External Threats

While the department has traditionally experienced strong economic support from the city budget, the economic downturn of the past three years has jeopardized funding levels for technology projects.

Internal Strengths

Police management has historically been supportive of the development and use of wireless technologies. Line level personnel, having been exposed to significant wireless technologies over the past 5 years, are receptive to new technology. An existing, robust, internal wired network provides support for existing and future wireless network connections.

Stakeholder Identification and Analysis

In order for strategic planning to succeed, it is necessary to identify the stakeholders, their concerns and their expectations as they relate to the goals of the plan. A stakeholder is a person or organization that has the potential to impact the outcome of, or is impacted by, the proposed change.

Users

Users are all employees accessing wireless applications as part of their job function. Users expect fast, convenient and reliable access to information and reliable wireless safety systems. Slow or unreliable networks or applications will increase workload and reduce safety. Generally, users are supportive of wireless technology changes that give them better and faster access to information. Users are likely to resist technology changes they do not understand the value of or that they perceive as intrusive.

Clients

Clients are persons and or organizations to which the department provides services. Clients expect the department to provide more effective and efficient police services using emerging technologies to increase service personnel availability in the field for fast response and crime suppression. Clients expect to be able to communicate easily with service personnel. The client's commitment to implementing wireless technologies is tied directly to the technologies ability to provide better service.

Vendors

Vendors are those commercial vendors who provide wireless service or wireless applications to law enforcement. Vendors have the ability to impact the availability and cost of wireless technologies available to law enforcement. Vendors have a high level of commitment to wireless technology implementations.

Police Management

Police management includes a chief of police, two captains, six lieutenants and one civilian manager. Police management expects wireless technology to provide more effective and efficient police services. Management expects wireless applications to make field personnel more accessible to the public by keeping them in the field and by providing a method for the public to directly communicate with field personnel. Cost, reliability, functionality and ease of maintenance are all critical factors to management.

City Manager

The City Manager must approve all technology projects and is concerned about cost versus benefit as well as reliability: and the benefit the technology will bring to the community.

Information Services Department

The Information Systems Department is tasked with implementing and maintaining wireless networks and applications. Reliability, ease of operation, user knowledge and vendor support are critical to maintaining systems. The Information Services Manager supports the strategic plan but is not yet committed to implementing the plan. It is critical for the Information Services Manager to actively support the implementation of wireless projects.

Governing body

The governing body for the City of Pleasanton is the elected City Council. The Council is concerned with providing the most effective and efficient police services at the

lowest cost to the community. The Council approves all funding and therefore has ultimate control over the implementation of wireless technologies. The Council has historically supported technology advances and currently has a neutral commitment level to implementing this plan.

Criminal Justice Information Agencies

State and federal Departments of Justice have regulatory authority over the use including wireless transmission of criminal justice and criminal offender record information. The implementation of networks or applications accessing criminal justice information must meet regulatory approval of these agencies. Criminal Justice Information Agencies are committed to providing information to law enforcement but no specific commitment to this plan.

Federal Communications Commission

The Federal Communications Commission controls the availability of radio spectrum. The availability of spectrum can have significant impact on which wireless technologies and services will be available to law enforcement and how they can be used. The Federal Communications Commission, by policy, is committed to providing public safety access to wireless spectrum but has no specific commitment to this plan.

American Medical Association

Surgeon General of the United States

The American Medical Association and the Surgeon General of the United States are generally considered the authorities on medical issues in the United States. The NGT panel pointed out that, while unlikely, a legitimate finding of electro magnetic interference (EMI) causing serious medical conditions could have catastrophic impact on the availability and use of wireless technologies. This type of finding would likely have to be supported by the American Medical Association or the Surgeon General of the United States to be considered legitimate. This issue has the potential of being a "snail darter" for this plan. A snail darter (Percina tanasi) is a small, rare fish discovered by a zoologist while snorkeling in the little Tennessee River upstream from the projected Tellico Dam. Dam opponents, fought successfully to include the darter on the Endangered Species List, halting construction of the dam.[xliii] The confirmation of a confirmed significant health risk from wireless devices has the potential to dramatically impact the ability of law enforcement to use wireless technology to meet future needs.

Development of Alternative Strategies

A number of approaches can be taken to meet the wireless data needs over the next five years. The department can continue to exist with its current first generation wireless technology, invest in and implement a private radio data network, invest in and implement a WiFi network, upgrade the current commercial system to third generation technology or take a multimodal approach combining two or more wireless networks in order to handle IP voice, data and video transmissions. In making this decision, the

department needs to consider which strategy will allow the agency to best meet its strategic goals, keeping in mind the critical expectations of stakeholders and availability of resources.

First Generation

Maintaining a first generation system is the least expensive solution. First Generation technologies while slow are capable of handling wide area network service and metropolitan area network service. These cellular systems are not designed to handle personal area network applications. Maintaining a first generation wireless network will jeopardize the agency's ability to meet its second goal, the implementation of leading edge wireless application technology. First generation wireless networks lack the speed and bandwidth necessary to meet the needs of emerging wireless applications and technology. While this solution would be the most economical, it does not meet the strategic goals of the agency.

Private Data Radio Network

The development of modern private radio data networks provides many advantages to law enforcement, no usage fees, control of the networks, interoperability and ownership of the spectrum. Cost of implementing private networks can be significant ranging from hundreds of thousands to millions of dollars depending on the size and geography of the coverage area. The cost of implementation and the availability of spectrum will likely force agencies to develop regional networks, with cost and usage shared by multiple agencies within a region. 700 MHz is the only dedicated spectrum

where public safety can have high speed wide area access to wideband data services such as voice IP, Internet applications and imaging.[xliv] Private data radio is a good wide area solution when spectrum becomes available. It appears unlikely that spectrum will become available in most large metropolitan areas for several years. While initial plans were to have television off the reallocated spectrum by 2006, this appears to be unlikely as current users can receive unlimited extensions based on the current state of digital transition in their particular market. The initial plans for reallocation of spectrum were predicated on the development and implementation of digital broadcast capabilities that has developed slower than planned.[xlv]

Third Generation Commercial

Upgrading the current first generation systems to faster third generation networks is a moderate cost solution. Initial investment for equipment is relatively low with commercial modems costing as little as $200 per unit and some carriers providing free modems. Service fees are dependant on usage, but generally run about $50 per month per unit. Third generation commercial systems are capable of handling wide area network needs and metropolitan area network needs. They are not designed to handle personal area network needs. Third generation networks have the speed and bandwidth to handle most of the emerging wireless applications and technologies. Some of these technologies, such as streaming video and voiceover IP, could significantly increase network usage and therefore have significant impact on service costs.

WirelessMAN

IEEE 802.16 wireless municipal area networks show great promise in reducing the initial cost of network implementation by reducing the number of access points needed. With data rates up to 75 Mbps and bandwidth of 20 MHz, 802.16 networks can provide services at the T-1 land line level. This technology is capable of handling both streaming video, voice over IP and data within the metropolitan area network. The weakness of this approach is the system's dependence on public spectrum and its limited range.

Preferred Strategy

Multimodal Network Approach

By taking a multimodal approach, the agency can combine the best attributes of different networks in order to meet its data, video and IP voice needs. Personal area networks, such as ultra wide band, allow personal and vehicle-installed electronic devices to communicate in real time without depending on offsite routers or access points. WirelessMAN networks are moderate installation cost, private networks, capable of providing metropolitan area coverage for data, video and IP voice. Commercial 2.5 and third generation networks are capable of covering gaps within the metropolitan area network and coverage outside the metropolitan network providing a moderately priced, reliable wide area network solution which meets law enforcement's data and telemetry needs. Using existing software applications or firmware such as software radio technology, these networks can be seamlessly integrated to provide a multimodal network

capable of handling the agencies data, voice and video needs at a moderate implementation, service and maintenance cost.

Implementation Plan

Goal #1 – Wireless Network Implementation

The Pleasanton Police Department will implement wireless network technology that will meet its wireless application needs for wide area networks, metropolitan area networks and personal area network applications.

Objectives

1. Implementation of a (3G) high-speed, high-bandwidth wide area wirelesses network service by 2007.
    a. Research private vs. public networks by 2005.
    b. Select network/vendor 2006.
    c. Develop network infrastructure 2007.
2. Implementation of a high-speed, high-bandwidth metropolitan area wireless network by 2009.
    a. Research and testing of available technologies, 2004/2005.
    b. Equip mobile computers with modems, 2006.
    c. Selection of hotspot vendor by 2006.
    d. Phase in implementation of hotspots, 2006-2009.
3. Implementation of Ultrawideband (UWB) wireless technology by 2009.

a. Research available technologies by 2006.

b. Test available technologies by 2007.

c. Identify and select vendors by 2008

d. Purchase and deploy hardware by 2009.

4. Continually evaluate effectiveness and update goal.

a. Yearly update of strategic plan.

b. Data sharing with other agencies.

c. Continued research.

Goal #2 – Wireless Application Implementation

The Pleasanton Police Department will implement wireless application technology that will provide field personnel with the tools to provide the community with more effective, efficient and safer policing services.

Objectives

1. Implementation of wireless streaming video capability by 2009

a. Research available technologies by 2006

b. Test available technologies by 2007

c. Identify and select vendors by 2008

d. Purchase and deploy hardware by 2009

2. Implementation of voice over IP by 2010

a. Research available technologies 2005/2006

b. Equip mobile computers with soundcards as part of replacement plan by 2005

c. Test available technologies by 2007

d. Select vendor by 2008

3. Implementation of wearable computer technology by 2010

a. Research available voice to text technologies by 2005

b. Test voice to text technologies in the mobile environment by 2006

c. Implement voice text technologies

d. Test available wearable hardware technologies by 2008

e. Identify and select short-range wireless technology by 2009

f. Select vendor in 2009

g. Implementation by 2010

4. Continually evaluate effectiveness and update goal

d. Yearly update of strategic plan

e. Data sharing with other agencies

f. Continued research

Implementing emerging wireless network technology will be critical for the agency and its clients. If a strong wireless network is properly implemented, it will provide the backbone needed to implement the plethora of emerging and future wireless applications that will significantly impact the work processes of law enforcement. The next chapter will identify strategies to overcome challenges and potential obstacles to

implementation of a multi-modal approach to upgrading wireless networks and applications.

CHAPTER IV

TRANSITION MANAGEMENT

Change Process

Simply identifying a vision, goals and a strategy for change does not create change in an organization. Creating major change in an organization can be a daunting task fraught with pitfalls and the ever, looming fear of failure. This can be especially true with technology projects in law enforcement organizations. Organizations must experience a cultural process in order to create change. The present state must be defrosted; a state of transition then occurs where change takes place; then a refreezing or anchoring in culture must occur. Each of these stages is critical to successful change.[xlvi]

This chapter will identify strategies to overcome challenges and potential obstacles to implementation of a multi-modal approach to upgrading wireless networks and applications.

.

Commitment Planning

Before change can be considered, there must be some internal or external driving purpose behind the change. If there is no obvious impetus for the change being suggested, then a sense of urgency must be established. If urgency is low, it will be difficult to establish a group with enough energy and credibility to guide the effort or to convince key players to spend the resources necessary to create the change.[xlvii] In order to implement the proposed change, it will be necessary to identify whose commitment is needed and what degree of commitment will be necessary.

A Commitment Plan is a series of actions steps designed to secure the support of those individuals and groups whose commitment is necessary to accomplish the strategic goals. The steps necessary for commitment planning are:

1. Identifying target individuals or groups (stakeholders) whose commitment is needed
2. Defining the critical mass necessary to ensure the effectiveness of the desired change
3. Development of a plan for getting the commitment of the critical mass
4. Creating a monitoring system to assess the progress[xlviii]

Commitment Charting

Stakeholders were identified in the strategic plan. This chapter will identify key stakeholders and define the commitment level necessary in order to ensure the implementation of the change using Commitment Charting. In order to implement any change, there is a minimum number of key stakeholders that is required to make change happen. These stakeholders are the critical mass.

Table 4-1 depicts commitment level of the critical mass with an X marking the current level of commitment and an O marking the minimum level of commitment needed from that stakeholder for the change to occur.

Table 4-1 Critical Mass Commitment Chart

Critical Mass	No Commitment	Let It Happen	Help It Happen	Make It Happen
Police Management				XO
City Manager	X			O
City Council	X		O	
Users	X	O		
IS Manager		X	O	

Strategies for Getting Commitment

City Manager

The City Manager currently has no commitment level. Support from the City Manager is critical obtaining funding and approval for wireless projects.

In order to accomplish the strategic goals, the City Manager must minimally help by approving the technology implementation and supporting the request for funding through the City Council. The following intervention strategies will be employed to create the conditions for commitment:

1. Support of the overall Strategic Plan that includes the wireless technology goals.
2. Use of cost benefit analysis.
3. Support from employee associations.

4. Invite the City Manager to attend technology demonstrations.

City Council

The City Council currently has no commitment level to this plan. In order to accomplish the strategic goals the City Council must minimally help by approving the technology implementation and providing funding. The following intervention strategies will be employed to create the conditions for commitment:

1. Use of cost benefit analysis
2. Seek support of the overall strategic plan that includes the wireless technology goals.
3. Use of public media to highlight current technologies and the advantages future technology could provide clients.
4. Support from employee associations.
5. Invite Council members to participate in ride-alongs, demonstrations and other programs designed to allow them to see the advantages of this type of technology.

Users

Wireless systems users currently have no commitment level to this plan Minimally the users must accept the technology in order for the goals to be implemented effectively. The following intervention strategies will be employed to create the conditions for commitment:

1. Provide necessary training to give users a working understanding of the technology.
2. Include users in the development of the strategic plan.
3. Include users as part of the selection and implementation committees.

Information Systems Manager

The Information Systems Manager is currently committed to helping implement this technology. Ultimately, the Information Systems Manager will have to be committed to implementing the goals of the strategic plan. The following intervention strategies will be employed to create the conditions for commitment:

1. Include IS Manager or representative in strategic planning.
2. Include IS Manager or representative in efforts to obtain funding.
3. Include IS Manager or representative in vendor selection process.
4. IS Manager to manage implementation of wireless technology.

Responsibility Charting

Responsibility charting is a technique used to clarify behavior that is required to implement important change tasks, actions or decisions. The technique helps reduce ambiguity, wasted energy and adverse emotional reactions between involved parties or stakeholders.[xlix] This technique will provide a road map identifying what responsibility each player has at each step in implementing the desired change.

The Responsibility Chart is a list of actions, decisions, or activities that affect the relationship between interrelated parties on the vertical axis and a list of identified involved actors on the horizontal axis. The involved actors include:

- Individuals directly involved in decision making
- Bosses of those involved
- Groups (board of directors, project teams, et cetera)
- People outside the organization (employee associations, controlling agencies, etcetera)

The required behavior of each participant is charted regarding any particular action or decision using the following classifications:

R Has responsibility for a particular action, but not necessarily authority.

A Must approve – has power to veto the action

S Must Support – has to provide resources for the action

I Must be informed or consulted before action, but cannot veto

- Irrelevant to the particular action

It is common to complete a Responsibility Chart for each goal. However, the wireless technology goals in this example are similar enough in process that one chart will do a good job of representing both goals. Restating the goals at this time will keep the responsibility chart in context to the sample strategic plan.

Goal #1 – Wireless Network Implementation

The Pleasanton Police Department will implement wireless network technology that will meet its wireless application needs for wide area networks, metropolitan area networks and personal area network applications.

Goal #2 – Wireless Application Implementation

The Pleasanton Police Department will implement leading edge wireless application technology that will provide field personnel with the tools to provide the community with more effective, efficient and safer policing services.

Table 4-2 Responsibility Chart

R Has responsibility for a particular action, but not necessarily authority.
A Must approve – has power to veto the action.
S Must Support – has to provide resources for the action.
I Must be informed or consulted before action, but cannot veto.
- Irrelevant to the particular action.

Decisions or Acts / Actors	City Manager	Chief of Police	City Council	IS Manager	Project Manager	Implementation Committee	Users	Employees Assoc.	Clients	Vendors	DOJ	FCC	Finance	Training Bureau
Planning	I	A	S	I	R	I	I	I	I	I	I	I	I	-
Funding	A	R	S	I	I	I	I	I	I	-	-	-	S	-
Research	-	I	-	A	R	R	I	I	-	S	-	-	-	-
Testing	-	I	-	A	R	S	I	I	-	S	I	I	-	-
Vendor Selection	A	A	A	S	R	R	I	I	I	S	-	-	I	-
Purchasing	I	I	-	S	S	I	-	-	-	S	-	-	R	-
Implementation	-	I	-	S	R	R	I	I	I	S	A	A	-	-
Training	-	I	-	S	S	I	S	I	-	S	-	-	S	R

Evaluating Success

Major change often takes a long time to implement. Technology, norms of behavior and shared values can change over time and therefore it is important to continuously evaluate the value and effectiveness of change throughout the process.[1] The strategic plan must contain provisions for reevaluating and redefining both goals and objectives on an annual basis. Strategic plans should be living documents growing and

changing to meet the needs of the organization and responding to the changing momentum of critical mass.

It is not difficult to critically evaluate whether or not goals and objectives were met. However, a true evaluation of the effectiveness of change requires the evaluator to evaluate the change in relation to the vision statement. In this case study, did the implementation of wireless networks and new technologies provide its mobile field work force untethered access to information in order to improve the efficiency, effectiveness and quality of services provided to clients and the safety of employees.

This type of value evaluation is much more difficult and requires time intensive gathering and analysis of information. The NGT group pointed out that the exponential technology curve has shortened the new technology life cycle making it difficult to properly evaluate implementations with traditional statistical methods. Evaluation and planning periods must become shorter. The agency must be willing to share data and experience with new wireless technologies between agencies and businesses in order properly evaluate new technology implementation in an environment of short life cycles.

The next chapter will summarize the conclusions of this research and provide some recommendations for police managers tasked with solving the wireless nightmare.

CHAPTER V

CONCLUSIONS AND RECOMMENDATIONS

Review

Law enforcement having long recognized the value of providing its mobile work force untethered access to the exchange of information has deployed wireless data networks since the mid 1970s. With the tremendous growth in the worldwide wireless communications industry, wireless technology is now capable of reaching hundreds of millions of people at virtually every location on the face of the earth. This growth in the marketplace has driven the development of wireless technology and applications. Deploying a mobile, information driven work force, law enforcement is poised to take advantage of this explosion of emerging technology.

As noted in Chapter 1 many law enforcement agencies in the United States are still using first generation private data radio and commercial analog data services ranging in speed from 4.6 kbs to 19.2 kbs. These systems are slow, antiquated and struggle to provide adequate service to existing applications. With the advent of personal computers, powerful servers and improved data networks, law enforcement has enjoyed a proliferation of software applications providing better access to data and improved work processes. Modern law enforcement agencies enjoy field access to integrated computer aided dispatch, records management, criminal justice databases, vehicle license databases and field reporting. A number of agencies are currently using their wireless networks to provide mapping and automated vehicle location using the Global Positioning System. A few law enforcement agencies have recently experimented

with wireless access to Internet applications such as California's system which allows law enforcement to access Department of Motor Vehicle photographs through the Internet.

Growth and changes in the wireless industry make it critical for law enforcement to have a strategic plan for wireless networking and technology development over the next 5 to 10 years. Internal and external forces are driving the critical mass necessary for law enforcement to commit to upgrading their wireless networks and technology. Agencies are being forced to upgrade wireless networks as vendors stop supporting old technology and begin to force agencies into newer technology that is less expensive for vendors to support and provides higher profits.

Law enforcement, a minor player in the wireless data market, does not drive the technology changes; therefore, it will be necessary for law enforcement to take advantage of market and technology changes to benefit its needs. Society's demand on law enforcement to increase service and performance will continue to drive the use of technology. The development of hardware and software will drive law enforcement to develop and implement supporting network backbones including wireless technologies. Law enforcement agencies will need to continue to meet government standards for the security of transmitted criminal justice information. International and domestic terrorism has created a push for law enforcement agencies to transition to protocols that will support interoperability between government agencies.

Law enforcement agencies must take on the task implementing wireless technologies for their agencies. The backbone of these projects will be the wireless and wired data networks needed to support the access to and sharing of data. Failure to plan

and act in the next five years will directly impact their ability to implement new hardware and software technologies over the next five to ten years. It is critical for agencies to investigate emerging technologies, develop a strategic plan to address future needs and transition their existing networks, hardware and software to wireless technologies that will meet their needs.

Recommendations

In answering the question of how a medium size urban law enforcement agency will use emerging wireless technologies to meet data transmission needs by 2009, it is necessary to define needs. As each agency is at a different evolutionary stage in its use and development of wireless technology, the example used in this research currently has modern applications in place and desires to implement new applications over the next five years.

Law enforcement will likely continue to use most of its current field applications. Three main categories of future wireless applications have been identified: streaming video, Internet Protocol based applications, and applications for personal data devices. These applications have bandwidth and speed requirements that will require law enforcement agencies to upgrade current wireless networks.

This paper has investigated the core of the plethora of wireless network technologies available today. These technologies fit into four basic categories, personal area networks (PAN), local area networks (LAN), municipal area networks (MAN) and wide area networks (WAN). These available and emerging private and commercial technologies each have a nitch in the marketplace. However, by themselves none of these technologies will meet the forecasted wireless needs of law enforcement. While

forecasts for fourth generation wireless networks show promise in meeting these needs, it is unlikely the marketplace will see these technologies available for 5 to 10 years.

Therefore, what should law enforcement agencies do while waiting for fourth generation technology to solve the problem? What strategy will best meet law enforcement's needs over the next five years and will help prepare the way for fourth generation implementation? What technology and what vendor should be selected?

Law enforcement management should consider taking a multimodal approach to developing wireless networks. Law enforcement's migration path should include the implementation of robust wide area wireless networks such as third generation commercial networks, metropolitan area networks such as WirelessMAN or private radio networks and personal area networks such as ultrawideband technology designed to function congruently. Wide area networks will provide the coverage necessary for agencies to function regionally. Metropolitan area networks will provide the ability to transmit large volumes of data, video and voice at high speeds without accumulating high usage fees. Personal area networks will provide the vital link between personal computing devices and wide area or metropolitan area networks.

Initially, these networks will integrate through software applications. As fourth generation firmware comes on the market, it is likely that seamless integration between networks of differing protocols will occur. A small number of innovative agencies have started down the path of multimodal networks using a combination of WANs and LANs.[li] These agencies have taken the first steps to creating fully integrated multimodal networks and will likely integrate municipal area networks and personal area networks as they mature.

What technology and what vendor should be selected in each network category? The answer to this question will be specific to the agency. Geographical availability, area geography, available resources, current networks, systems compatibility, existing services and contracts are all issues that are specific to each agency. A good selection process should take all of these issues into consideration when selecting vendors for services or equipment. The multimodal approach to meeting wireless data needs is an open architecture solution allowing agencies to select vendors and technology that meets their individual needs while building an integrated network that will likely handle their needs for 5 to 10 years.

Navigating the Wireless Nightmare

In the first four chapters of this paper, existing, emerging and future technologies were researched; future events and trends impacting the issue were examined; and sample strategic and transition plans were presented. All of this to answer the simple question: "How will emerging technologies be used by a mid-size urban law enforcement agency to address wireless data transmission needs by 2009?" After completing this research, no single wireless solution was identified that will meet all of the projected needs of the agencies in the target group. Combining different wireless technologies to form multimodal integrated networks, which will support the variety of applications law enforcement will likely be implementing, is the best solution for the next five years. Based on the lessons learned in this exercise, some recommendations can be made to those tasked with solving the wireless nightmare:

- Agency heads should remain active in encouraging legislation and regulatory rulings advantageous to law enforcements use of wireless networks.
    - Encourage the release of 700 MHz spectrum to public safety.
    - Encourage legislation requiring public wireless service to provide priority access to public safety.
- Be inclusive when seeking input for planning, selection and implementation of wireless projects
- Provide adequate training to all users
- Develop internal experts capable of planning, managing and monitoring wireless technology
- Seek and share information with other users of wireless technology
- Avoid implementation of proprietary protocol applications and technologies. Standard protocol technologies will provide an easier transition to third and fourth generation networks
- Anticipate short lifecycles for wireless technology over the next ten years
- Do not fall victim to analysis paralysis, life cycles for wireless technology are too short
- Budget for continuous research and development of new technologies
- Research and test new technologies, implement proven technology

The use of technology must be an integral part of the vision of the organization. Police managers must continually look to the future of the organization and be willing to embrace the rapid change in work processes that wireless technology has brought and

will continue to bring to the law enforcement industry. Failure to plan and act will leave agencies in a technology void. They risk losing their current networks and applications, failing to have any input into new technologies, failing to meet regulatory requirements and failure to provide value added services and improved work processes to employees and clients.

APENDIX I
NGT GROUP

Facilitator

Mark Senkle	Police Lieutenant	Pleasanton Police Department

Scribe

Lisa Mezzetti	Community Service Officer	Pleasanton Police Department

Observer

Briuce Barsi	Police Captain	Mountain View Police Department

Panel Members

Kathy Carlson	Account Manager	Atlantic Telephone and Telegraph
Eric Finn	Police Lieutenant	Pleasanton Police Department
Allen Hammond	Information Systems Director	City of Pleasanton
Bruce Johnston	Engineer	Atlantic Telephone and Telegraph
Doug Kiner	Information Systems Technician	Mountain View Police Department
Bill Lim	Computer Programmer	W. Covina Services Group
Kathy Small	Account Manager	Cisco Systems

APPENDIX II
NGT EVENTS LIST

The following is a list of all events identified by the NGT Group:

1. Energy Company approved by FCC to provide broadband service.
2. One hundred megabit wide area network deployed.
3. Identity chip mandated for wireless devices
4. Courts restrict ability of law enforcement to share information between jurisdictions.
5. New patriot act repeals privacy rights.
6. Major wireless providers merge.
7. Hacker compromises state database thru wireless connection.
8. State mandates inoperability between all databases.
9. Motorolla gets tough and inters the commercial wireless market.
10. Microantennas developed for cell sites
11. Agency sued over violation of privacy after using wireless surveillance.
12. Digital video recorders in patrol vehicles reaches 50% penetration.
13. Scientists prove electro magnetic interference causes brain cancer.
14. Federal Government requires all local agencies to meet new wireless security standards.
15. Terrorism act on a national communications network.
16. DOJ approves Internet use for criminal offender information.
17. FCC re-allocates spectrum to public safety.
18. City bans all new cell sites.
19. Federal Government requires wireless carriers to provide public safety priority access.

APPENDIX III
NGT TREND LIST

The following is a list of trends identified by the NGT group:

1. Amount of technical knowledge of employees
2. Commitment level of vendors to public safety service levels.
3. Amount of government enterprise into wireless industry.
4. Availability of wireless field applications
5. The number of vendors in the wireless service market.
6. Cost of maintaining technology.
7. Number of government mandates on public safety's use of wireless technology.
8. Level of quality of wireless service.
9. Availability of wireless field hardware.
10. Level of data security.
11. Degree of standardization in the wireless industry.
12. Degree of concern the public has over privacy.
13. Amount of funding available for technology projects.
14. The amount of radio spectrum available.
15. The degree of government regulation of radio spectrum availability.
16. The geographical availability of wireless networks.
17. Degree to which field officers will use wireless field technology.
18. Degrees of interoperability between government agencies.
19. The number of vendors offering consolidated wireless services.
20. The availability of bandwidth.
21. Cost of airtime on commercial networks.
22. Cost of deployment of wireless network technology.
23. The number of emerging and new wireless technologies available.
24. The amount of convergence between voice, digital video and data.
25. The degree of public acceptance of wireless technology.
26. Availability of microtechology.
27. The length of period in wireless technology lifecycles.
28. Availability of firmware designed to allow users to connect to multiple networks.

ENDNOTES

---

[i]Daniel L. Lough, T. Keith Blankenship, Kevin J. Krizman , "A Short Tutorial on Wireless LANs and IEEE 802.11" (The Bradley Department of Electrical and Computer Engineering Virginia Polytechnic Institute and State University Blacksburg, Virginia), 1.

[ii] Jim Chu, "Law Enforcement Technology Tutorial – The ABC's of IT" (lecture presented IACP Law Enforcement Information Management Training Conference, Sacramento, 3 May 2004).

[iii] Ibid.

[iv] Barbara Montgomery, "Commercial Wireless Technology Comparison" (lecture IACP Law Enforcement Information Management Training Conference, Sacramento, 4 May 2004).

[v] "About Mobile Technology and IMT-2000" [online article], (accessed 13 December 2003); available from http://www.itu.int/home/index.html About Mobile Technology and IMT-2000; Internet: 1.

[vi] Chetan Sharma, Yasuhisa Nakamura, "Wireless Data Services," Cambridge University Press, 2003, 116-117.

[vii] Ibid,. "About Mobile Technology andIMT-2000".

[viii] Ibid.

[ix]" Enabling Technologies" [online article], (accessed 13 December 2003); available from http://www.nortelnetworks.com/corporate/technology/wireless/protocols/html; Internet: 1-3.

[x] Ibid.

[xi] Ibid.

[xii] Ibid.

.

[xiii] "GSM & GPRS Based Telematics & AVL, GPRS Overview" [online article], (accessed 13 December 2003); available from http://www.webtechwireless.com/gsm-gprs-telematics.htm; Internet: 1-3.

[xiv] Ibid.

[xv] Enabling Technologies, 1-3.

[xvi]Ibid., Chetan Sharma, Yasuhisa Nakamura, 311-312.

[xvii] Ibid., 311-312.

[xviii] Ibid., http://www.weca.net/opensection/glossary.asp?TID=2 pg.1.

[xix] Jon Fortt , "Research Forum Leader Takes On Wireless Challenge," Mercury News and Wire Services, 15 December 2003, available from http://www.silconvalley.com; Internet.

[xx] Ibid., Chetan Sharma, Yasuhisa Nakamura, 311-312.

[xxi] Ibid., 295.

[xxii] "700 MHz TV Clearing, its Impact on TV Viewership, and Options for Accelerating Public Safety Access" [white paper], (Motorola, Inc., 2 February 2004); available from http://www.motorola.com; 5.

[xxiii] Ibid., 6.

[xxiv] Ibid., 9,10.

[xxv] Ibid., http://www.weca.net/opensection/glossary.asp?TID=2 pg.1.

[xxvi] "WiFi" [online article], (accessed 15 December 2003); available from http://www.pcwebopedia.com/TERM/W/Wi_Fi.html; Internet: 1.

[xxvii]"Popular Wireless Local Area Networks Gain Large Boost in Speed" [online article], (Institute of Electrical and Electronics Engineers, 20 June 2003); available from http://standards.ieee.org/announcements/80211gfinal.html; Internet: 2
.

[xxviii] Ibid., http://www.weca.net/opensection/glossary.asp/TID=2; pg.1.

[xxix] "Enterprise Solutions for Wireless LAN Security"[white paper online], (2003 Wi-Fi Alliance, 6 February 2003); available from http://www.WiFialliance.org; Internet; 2.

[xxx] Ibid., 5.

[xxxi] Daniel L. Lough, T. Keith Blankenship, Kevin J. Krizman , "A Short Tutorial on Wireless LANs and IEEE 802.11", 3.

[xxxii] "IEEE 802.16 and WiMAX – Broadband Wireless Access for Everyone" [white paper online], (Intel, 2003); available from ww.wimaxforum.org; Internet; 2,3.

[xxxiii]"The DataStorm – Mobile Internet Anywhere" [online white paper]; available at www.groundcontol.com/mobile_001.htm; Internet; accessed 15 December 2003; 1.

[xxxiv] Ibid., Chetan Sharma, Yasuhisa Nakamura, 189-191.

[xxxv] Ibid., "Wireless LAN Standards", 1,2
.

[xxxvi] Ibid., Chetan Sharma, Yasuhisa Nakamura, 314-315.

[xxxvii] Ibid.,188-191.

[xxxviii] Ibid., 315,317.

[xxxix] Ibid., 3.

[xl] Ibid.

[xli] Ibid., 310,311.

[xlii] Tom Esensten, OEC, Lecture Dec 2003.

[xliii] Columbia Encyclopedia, sixth edition, [online encyclopedia], (accessed 6 June 2004); available from http://www.columbiaencyclopedia.com; Internet.

[xliv] "Motorola Officer Full Suite of 700 MHz Technology Vital to Mission-Critical Public Safety Interoperability" [on-line press release], (accessed 13 April 2004); available from http://www.motorola.com/LMPS/pressreleases/page3180.htm; Internet, 1-2.

[xlv] Ibid, "700 MHz TV Clearing, its Impact on TV Viewership, and Options for Accelerating Public Safety Access";6.

[xlvi] John P. Kotter, Leading Change Executive Summary, Harvard Business School Press, 1996,1.

[xlvii] Ibid., 36.

[xlviii] Ibid., 93.

[xlix] Ibid.

[l] Ibid., John P. Kotter,148.

[li] "WLAN technology protects and serves", NetworkWorldFusion, [online article], (accessed 3 February 2003), available from http://www.nwfusion.com/news/2004/0126 wireless.html; Internet, 1-3.

700 MHz TV Clearing, its Impact on TV Viewer ship, and Options for Accelerating Public Safety Access. White paper. Motorola, Inc., 2 February 2004; available from http://www.motorola.com; Internet.

About Mobile Technology and IMT-2000. 2003. On-line article. Available from http://www.itu.int/home/index.html About Mobile Technology and IMT-2000; Internet.

DataStorm, the – Mobile Internet Anywhere. 2003. White paper. Available at www.groundcontol.com/mobile_001.htm; Internet.

Enabling Technologies. 2003. On-line article. Available from http://www.nortelnetworks.com/corporate/technology/wireless/protocols/html; Internet.

Enterprise Solutions for Wireless LAN Security. 6 February 2003. White paper on-line. Available from http://www.WiFialliance.org; Internet.

Esensten, Tom. Startegic Planning. Oxnard: Lecture presented at Command College Class 36, Dec 2003.

Fortt, Jon. "Research Forum Leader Takes On Wireless Challenge," Mercury News and Wire Services (15 December 2003). Available from http://www.silconvalley.com; Internet.

GSM & GPRS Based Telematics & AVL, GPRS Overview. 2003. On-line article. Available from. http://www.webtechwireless.com/gsm-gprs-telematics.htm; Internet.

IEEE 802.16 and WiMAX – Broadband Wireless Access for Everyone. 2003. Intel White paper. Available from http://www.imaxforum.org; Internet.

Kotter, John P. Leading Change Executive Summary. Boston: Harvard Business School Press, 1996.

Lough , Daniel L., T. Keith Blankenship, Kevin J. Krizman , "A Short Tutorial on Wireless LANs and IEEE 802.11", Blacksburg : Virginia Polytechnic Institute and State University, 2002.

Motorola Officer Full Suite of 700 MHz Technology Vital to Mission-Critical Public Safety Interoperability. 12 August 2003. On-line press release. Available from http://www.motorola.com/LMPS/pressreleases/page3180.htm; Internet.

.

Bibliography

Popular Wireless Local Area Networks Gain Large Boost in Speed. 20 June 2003. On-line article. Institute of Electrical and Electronics Engineer. Available from http://standards.ieee.org/announcements/80211gfinal.html; Internet.

Sharma, Chetan, and Yasuhisa Nakamura. Wireless Data Services. New York: Cambridge University Press, 2003.

WiFi. 2003. On-line article. Available from http://www.pcwebopedia.com/TERM/W/Wi_Fi.html; Internet.

WLAN Technology Protects and Serves. 2003 On-line Article. Network World Fusion. Available from http://www.nwfusion.com/news/2004/0126 wireless.html; Internet.