Research Report

BOB HARRISON, JAMES DIMAROGONAS, JARRETT CATLIN, RICHARD H. DONOHUE,
THOMAS GOUGHNOUR, JOHN S. HOLLYWOOD, JASON MASTBAUM,
KRISTIN VAN ABEL, JAY BALAGNA

Broadband Communications Prioritization and Interoperability Guidance for Law Enforcement

Critical Considerations in the Transition to the Public Safety Broadband Network

For more information on this publication, visit **www.rand.org/t/RRA2019-1**.

About RAND

The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest. To learn more about RAND, visit www.rand.org.

Research Integrity

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Published by the RAND Corporation, Santa Monica, Calif.

Library of Congress Cataloging-in-Publication Data is available for this publication.

ISBN: 978-1-9774-0992-8

Cover photo: First Responder Network Authority.

Limited Print and Electronic Distribution Rights

About This Report

The U.S. Department of Justice, Office of Justice Programs, National Institute of Justice (NIJ) solicitation 2018-14046 sought research and evaluation projects to develop practical knowledge that would inform the deployment of mobile broadband communications technologies by law enforcement agencies, to identify state and local agencies leading in the deployment of these technologies, to study existing and conceptual network architectures, to evaluate operational deployments, and to synthesize the results into a guidance document. The RAND Corporation's Engineering and Applied Sciences department conducted this work. Although the coronavirus disease 2019 pandemic delayed work because of the inability of law enforcement organizations to devote time to respond to research and interviews in lieu of conducting critical field operations through most of 2020, the delay provided an extended period in which to evaluate the deployment of the National Public Safety Broadband Network (NPSBN) and the efforts by other broadband vendors to market similar services, as well as the NPSBN's expansion of FirstNet as a part of its build-out of that platform. This report serves as the guidance desired by NIJ for law enforcement and first responders as they transition to the NPSBN or elect to deploy mobile broadband services for their communities.

Justice Policy Program

RAND Social and Economic Well-Being is a division of the RAND Corporation that seeks to actively improve the health and social and economic well-being of populations and communities throughout the world. This research was conducted in the Justice Policy Program within RAND Social and Economic Well-Being. The program focuses on such topics as access to justice, policing, corrections, drug policy, and court system reform, as well as other policy concerns pertaining to public safety and criminal and civil justice. For more information, email justicepolicy@rand.org.

Acknowledgments

This research was supported by the National Institute of Justice through contract 2018-75-CX-K001. We thank Scott Edson, executive director of LA RICS, who served both as an expert resource on the future of interoperable radio and FirstNet and as a reviewer of the final report. We also thank members of law enforcement agencies that partnered with us during the execution of this research, particularly Chief of Police (Ret.) Keith Kauffman of the Redondo Beach Police Department, who provided an executive perspective on the future of consolidated radio systems for municipal policing; Deputy Chief Sarkis Ohannessian of the San Bernardino County Sheriff's Office, who facilitated discussions with staff and county subject-matter experts; Jade Mazzio, business services manager at the Irvine Police Department, who gave insights into the ways in which regional radio and broadband networks will affect dispatch, records, and operational systems; and Ray Edey, executive director of ICI Systems, in Glendale, California, who provided insights into the administration and future of interdisciplinary communications systems for police, fire, and emergency medical services. We also thank Andrew Seybold, chief executive officer of Andrew Seybold, Inc., a pioneer in mobile broadband, who generously gave his time to discuss FirstNet. This report would not be possible without input from many stakeholders across multiple law enforcement and emergency responder agencies, service providers and equipment manufacturers, researchers, and federal government agencies. We truly appreciate their time and candor. We thank the many individuals within RAND who support the research that we do and who helped with the preparation of the final report. We would also like to thank Tim Bonds for his thorough review and comments, which greatly improved this report. Finally, we thank Cathy Girouard and Joseph Heaps from the National Institute of Justice for their tremendous support and invaluable advice throughout the process.

Summary

"I just want it to work," said one of many law enforcement representatives whom we interviewed about their use of broadband for first responders. This statement summarizes the sentiments of many end users: No matter the technology, no matter how land mobile radio (LMR) and mobile broadband are configured, all they want is for someone to hear them when they call for help.

After years of dialogue, the creation of a federally funded and managed public safety broadband network in 2012 was supposed to result in simple solutions for those seeking interoperability. For various reasons, this has not happened. In this report, we seek to provide guidance for first responders so that they can make the best possible decisions for their agencies.

To address the dizzying array of providers, capabilities, and options for the future, we aim to inform agencies about available broadband options and opportunities, issues of governance, funding options, costs, and barriers to implementation. This report is intended to help law enforcement executives, their staff, and their city or county communications technology providers chart a course forward that optimizes what they have now while also establishing processes to better integrate technologies for enhanced interoperability from officer to officer, agency to agency, and discipline to discipline.

Background

2018 marked the first year that law enforcement agencies had access to a nationwide, interoperable first responder broadband communications network, the federally created National Public Safety Broadband Network (NPSBN), called FirstNet (FirstNet.gov, undated b). FirstNet is federally regulated through the First Responder Network Authority, an independent authority within the U.S. Department of Commerce created in 2012 (FirstNet.gov, undated b). At the time that FirstNet's commercial contractor, AT&T, came online, competing broadband communications alternatives also emerged from commercial broadband companies that sought to provide similar services to law enforcement customers, such as a private core for enhanced security and service management, preemption and prioritization for public safety in times of emergency, and interoperability across broadband platforms. All 50 states and five U.S. territories opted to use FirstNet rather than sponsor their own networks.

Broadband communications for law enforcement are significantly augmented by this national public safety network; however, the opportunity to communicate more effectively via broadband (Carter, Grommon, and Franz, 2014) introduces additional complexity and operational limitations. In particular, in considering a transition to FirstNet, law enforcement agencies are faced with complex trade-offs to acquire, manage, and use these broadband communications networks while maintaining critical LMR and radio dispatch legacy systems (Favraud et al., 2016).

Key Findings

As described in this report, the acquisition, use, and sustainment of a broadband communications system for use in law enforcement requires careful consideration of the following issues.

Available Communications Technologies and Providers

There are many device options and service providers available and many systems that make up a law enforcement and emergency responder network. The network architecture can include a variety of cellular providers, backhaul providers, LMR, and gateways and interconnect points to bring all of these different systems together.

Governance

Governance is needed to establish clear lines of authority and priorities for investment and to support the functional operation of a system. To ensure the effective deployment and operation of a communications system, all governance bodies should have documented authority related to official plans and resolutions, active and accountable membership, frequent and consistent meetings, and regular planning for emerging scenarios (SAFECOM and National Council of Statewide Interoperability Coordinators, 2018). Use cases can help identify an agency's specific requirements for communications technologies.

Funding and Acquisition

Agencies have multiple options for funding communications technologies, including dedicated information technology budgets, police or municipal annual or operating budgets, grants, and private donations. One option for the acquisition process is to address the following five steps: needs identification, market research, purchasing, implementation and maintenance, and legacy disposal.

Costs

Budgeting for broadband communications covers a large number of costs, including software apps, connections between mobile apps and back-end databases, mobile device management systems, mobile application management systems, bridging to LMR networks, training, and personnel (both to oversee fielding and maintenance and to oversee software and network administration). The type of network provider selected—a single network provider, a dual-provider option, or a single provider with an integrated LTE (Long-Term Evolution)/LMR device—is a decision that involves considerable costs, not only to the expense of acquiring and maintaining a communications platform but to the infrastructure of the agency in terms of materiel costs, replacement cycles, and periodic upgrades to hardware and software systems.

Key Considerations

Moving forward, there are three key considerations of which decisionmakers should be acutely aware—during the acquisition phase, in which products and services are identified and systems contracted; in daily and emergency use; and as ways to manage any system are contemplated.

System Reliability

When officers, firefighters, or paramedics push buttons on their mobile devices, do the persons with whom they intend to communicate hear them? Is the coverage for such devices adequate, or are there gaps in coverage that could threaten lives or safety in an emergency? What metrics of reliability should be used to gauge an acceptable level of service for various needs and circumstances? One critical aspect of reliability is the ability of a communications system to interoperate smoothly with other systems. Rather than presuming that one platform can "talk" with others or relying on patchwork solutions, agencies should determine the present and future reliability of proposed systems, both now and in the future, at the time that a technology provider is selected.

System Survivability

FirstNet seeks to be "public safety grade" and should be able to survive the various natural and human threats to survivability, including wildfires; active shooter events; multiagency responses saturating networks; and weather events, such as hurricanes, tornadoes, intense rainfall, and earthquakes. However, there is no standardized definition of "public safety grade." Depending on geography, topography, and recurring vulnerability to weather phenomena, agencies might already know the most likely and foreseeable threats to their broadband infrastructure. Any system that is employed for public safety broadband communications should be oriented to survive in those circumstances and also survive any novel threats that might emerge.

System Governance

Although agencies traditionally manage broadband contracting, equipment, and deployment individually, the nature of an increasingly connected world might mean that economies of scale, interoperability issues, and policy conformance would be better served within the structure of a *joint-powers authority*, a consortium dedicated to communications capabilities or similar governance structure. Although FirstNet/AT&T, Verizon, and others might state that their technology and broadband platforms are the best means by which to ensure desired outcomes for public safety, they are on differing broadcast bands and use different equipment while offering similar capabilities. Law enforcement agencies must ask for clear, specific details before contracting for service. Those details should include coverage capabilities (present and planned); system survivability; system adaptability, especially to incorporate desired functionalities or public safety applications; and performance metrics that agencies can use to gauge compliance with any contracted services.

Conclusion

When considering the transition to the NPSBN or another broadband platform, decisionmakers must choose their path forward knowing the specifics of the proposed technology and how it will perform in the real world. It is incumbent on the agency decisionmakers seeking those elements of their communications platform to act only when they have articulated the specific performance, support, and development of whatever choice they make.

Contents

CHAPTER SEVEN

CHAPTER EIGHT

APPENDIXES

Figures and Tables

Figures

Tables

CHAPTER ONE

Introduction

Background

On February 22, 2012, Congress signed into law the Middle Class Tax Relief and Job Creation Act of 2012, which established a nationwide, interoperable public safety broadband network—the National Public Safety Broadband Network (NPSBN)—and mandated that the Federal Communications Commission (FCC) reallocate the 700-megahertz (MHz) D block spectrum (20 MHz of "prime" spectrum) to this network for use by public safety entities only (Pub. L. 112-96, 2012). The law also established an independent authority, the First Responder Network Authority, or FirstNet,[1] charged with deploying and operating the NPSBN (Pub. L. 112-96, 2012). The NPSBN is intended to fill a critical gap to achieve seamless communication across first responder jurisdictions carrying out law enforcement, fire, or emergency medical services (EMS) through dedicated physical infrastructure and the use of technology (hardware and software).

FirstNet was allocated $7 billion for the build-out of the NPSBN (Pub. L. 112-96, 2012, Section 6413(3)) and given the authority to execute the mandate with grants or contracts with "individuals, private companies, and Federal, State, regional, and local agencies" (Pub. L. 112-96, 2012, Section 6206(b)(4)(A)). In March 2017, FirstNet awarded a 25-year contract to AT&T to build the NPSBN (FirstNet.gov, undated b). The broad terms of this public-private partnership include performance-based payments of $6.5 billion from FirstNet to AT&T over the first five years of the contract to support the build-out of the network; AT&T investment on the order of $40 billion over the term of the contract to build, operate, and maintain the network; and access to AT&T's existing telecommunications network and assets for FirstNet subscribers (FirstNet.gov, 2017).

Even though AT&T became FirstNet's contracted partner to build and operate the NPSBN, other broadband service providers have deployed dedicated public safety broadband services that are similar to FirstNet—although these are not governmentally managed except through FCC and related federal communications laws—and are competing for a share of the public safety broadband market. This has caused considerable confusion for end users (e.g., law enforcement, fire services, emergency management services, and related public safety entities) because the available options on the marketplace are seemingly very similar. Furthermore, many of the potential FirstNet end users have existing, commercially available broadband services,[2] and the costs and benefits of transitioning to a dedicated service or network, either with their existing provider or with another provider, can be opaque. Agencies must expend public funds to transition to the

[1] The First Responder Network Authority resides within the National Telecommunications and Information Administration of the U.S. Department of Commerce. FirstNet is headed by a board that consists of "(A) the Secretary of Homeland Security; (B) the Attorney General of the United States; (C) the Director of the Office of Management and Budget; and (D) 12 individuals appointed by the Secretary of Commerce in accordance with paragraph (2) [of the Act]" (Pub. L. 112-92, 2012, Section 6204).

[2] In interviews with law enforcement, fire, and emergency management services agencies, we learned that many agencies contract with the large, nationally known telecommunications companies, such as AT&T and Verizon, but that some also

NPSBN, contract for public safety broadband with another provider, or remain in a status quo position until they can be confident choosing how to provide broadband to their respective officers, deputies, firefighters, and emergency services personnel.

Complicating issues of cost, determining when to switch to the NPSBN or other public safety network or service, how to conduct the transition, and what services and capabilities are necessary to perform agency-specific duties requires a good understanding of the technical differences between available broadband options. Some agencies do not possess this capability in house and therefore need assistance understanding the difference between Long-Term Evolution (LTE), 4G, and 5G, for example.

Purpose of This Report

To address the dizzying array of providers, capabilities, and options for the future, this report is intended to help agencies make informed decisions regarding the purchase, fielding, and integration of broadband communications into operations. We seek first to inform the end user of available broadband options and opportunities and to help demystify the myriad capabilities of the NPSBN and competing broadband platforms. We then address issues of governance, funding, costs, and barriers to implementation.

The report is intended to help law enforcement executives, their staff, and their city or county land mobile radio (LMR)/LTE providers chart a course forward that optimizes what they have now while also establishing processes to better integrate both technologies for enhanced interoperability from officer to officer, agency to agency, and discipline to discipline. It also contains a glossary and explanations of the various generations of broadband service to further clarify the present, the planned future, and possibilities beyond.

In the remainder of this introduction, we provide a brief overview of the ways in which broadband can serve as an enabler of law enforcement capabilities and introduce some key questions to be asked when acquiring a broadband capability.

Broadband as an Enabler of Law Enforcement Capabilities

In an increasingly connected world, trying to deliver policing services without adopting a broadband platform to deliver the speed and reliability of current and emerging technologies will put an agency behind the demands of both its officers and the public they serve. Examples of capabilities that can be enabled or enhanced with broadband networks include

- sharing identifying information and criminal history data at a much higher rate of speed than previously possible
- receiving and sharing critical law enforcement alerts, including alerts to field units as they transmit identifying information for vehicles or people of wanted status, and other officer safety data in close to real time
- receiving and sharing video streams from body-worn cameras, site surveillance cameras, unmanned aerial vehicles (UAVs), and unmanned ground vehicles (UGVs)
- communicating on shared digital voice channels via smartphones, using push-to-talk (PTT) functionality in a manner similar to LMR platforms

contract with local or regional service providers. We discuss interview findings throughout the report but primarily in Chapters Four through Six.

- prioritizing law enforcement and public safety broadband devices on selected bandwidth to ensure continuity of communications during emergencies through over-the-top PTT (OTTPTT) or "mission-critical" PTT (MCCPTT)
- enabling interoperability within a given jurisdiction's public safety agencies and across jurisdictions to provide seamless communications in conducting law enforcement, fire, and EMS duties.

To achieve these capabilities, a law enforcement agency must acquire broadband devices for use by all or select members of the agency, field the networks, and integrate devices into its existing communications platforms and protocols. Although policing agencies have commonly acquired devices and platforms individually (often through city or county purchasing systems or LMR collaboratives), there are alternatives that can be more effective both to acquire and to then use LTE and emerging 5G devices and networks. Individual agencies can share various resources related to law enforcement communications through joint-powers agreements to establish and manage LMR frequencies, to consolidate public safety answering point (PSAP) dispatch centers, to share automated data and criminal history information, and to conduct related data-sharing that could be affected by changes in LMR/LTE communications. An agency might also work in partnership with a larger agency (like a county sheriff's department) to manage LMR/LTE services under a contract with other member agencies.

Questions to Ask in Considering Acquisition of a New or Modified Broadband Capacity

Law enforcement agencies that are considering a new or modified broadband capacity should ask themselves the following broad questions during the decisionmaking process.

Governance Questions

What governing structures and policies exist or need to be developed that would enable the agency

- to acquire, deploy, and manage an interoperable law enforcement broadband network for its jurisdiction?
- to integrate broadband operations with adjacent and regional public safety agencies?
- to evaluate how existing joint-powers agreements might be affected by these changes?

Technology Questions

- Which broadband networks meet the needs of the agency according to the envisioned future operational state (including coverage capabilities and hardware and software reliability requirements)?
- Which devices are best suited to accomplish the coverage and interoperability requirements of the jurisdiction and its environs?
- What law enforcement–specific applications will be necessary to create the functionality required to deploy a PSBN effectively?
- Who will be responsible for device management, both mobile devices and the mobile applications installed to provide the functionality desired?
- What network management tools are included with the broadband service that support leadership intent and allow policies to be enacted and sustained?

- Does the service provider have a road map that provides gateway solutions to incorporate LMR/LTE solutions into existing LMR/PSAP infrastructure?
- How will emerging capabilities of 5G networks affect the continued transition away from legacy communications systems to a network that offers desired communications systems?

Business Management and Process Questions

- Who will be responsible for device management, both mobile devices and the mobile applications installed to provide the functionality desired?
- What are the existing processes for acquiring new or upgraded devices and infrastructure?
- How will the agency fund ongoing operations and maintenance, upgrades, and continued development of the LMR/LTE system?

Organization of This Report

The remainder of this report is organized as follows:

- In Chapter Two, we discuss our approach and methodology for this study.
- In Chapter Three, we describe in detail the core broadband communications technologies, network assets, and architectures, including a brief history of the transition from narrowband to broadband (1G to 4G), 5G and emerging advances, and mobile assets.
- In Chapter Four, we discuss governance and operational requirements.
- In Chapter Five, we cover funding, acquisition, and maintenance.
- In Chapter Six, we outline cost elements and rough order-of-magnitude costs associated with the purchase and integration of devices and infrastructure.
- In Chapter Seven, we discuss three primary barriers to an effective transition to future broadband capabilities. We also present voices from the field to reflect the perspectives and concerns of end-user agencies.
- In Chapter Eight, we offer conclusions and key takeaways for the reader. We also present a story of the possible future of public safety broadband and its uses in 2042 to help the reader visualize the possibilities ahead.
- In Appendix A, we provide a deeper discussion of broadband technologies.
- In Appendix B, we present a set of "coverage maps" for select communications areas.
- In Appendix C, we provide a glossary.

CHAPTER TWO

Methodology

In this chapter, we present the methodology we used in this analysis. We relied on literature reviews and interviews with subject-matter experts (from law enforcement agencies, technology and service providers, and other industry and government personnel) to collect information about available broadband offerings; the technical specifications of telecommunications technology and applications; existing governance; funding and acquisitions processes and mechanisms that law enforcement agencies use for telecommunications infrastructure; and costs associated with the purchase and integration of devices and infrastructure. We also discuss the limitations of this study.

Literature Review

We conducted an extensive literature review on the topics of broadband communications and related technologies, their application to law enforcement and emergency responders, and the acquisition and management of such networks.

Subject-Matter Expert Elicitations

In parallel, we used several methods for expert elicitations from technology subject-matter experts, law enforcement practitioners, service providers, and law enforcement network managers to get a broad set of perspectives. These expert elicitations were conducted through meetings, workshop and conference participation, electronic contacts, and in-person interviews.

We conducted in-person interviews with experts from the four agencies that agreed to participate in the project, inquiring into

- their current state of LMR and LTE deployment for police and fire resources
- the vendor or vendors used to supply broadband hardware and software
- the manner in which broadband resources are financed for the police within their jurisdiction
- any joint-powers agreement or consortium they participate in for either LMR or LTE
- any issues with connectivity for broadband public safety uses in normal operating circumstances
- any issues with the same connectivity during emergencies, multiagency responses requiring interoperability, or planned large-scale events
- any plans to migrate to the NPSBN through contracting with ATT/Firstnet.com
- the underlying rational for migration to a new broadband service provider or platform; conversely, the rationale for remaining in their present broadband service configuration.

We also conducted an online assessment of more than 30 policing agencies in California and Massachusetts using a structured query instrument to determine the status of, planned future of, and issues with broadband for these organizations. A number of the agencies surveyed were contacted via telephone to clarify responses and complete areas where answers were seen as missing or incomplete.

Development of Coverage Maps for Select Communications Areas

We completed a set of "coverage maps" for select communications areas to present the limitations of communications for LTE networks so that public safety agencies can better understand the different ways that LTE, 5G, and LMR provide *coverage* (a reliable frequency availability to sustain communications among mobile devices and base stations [for LMR]).[1] These maps are presented in Appendix B, where the reader will see the following:

- Among the four LTE frequencies (778 MHz, 850 MHz, 1,900 MHz, and 4 gigahertz [GHz]), the coverage is similar and does not significantly improve from one frequency to another.
- As frequencies rise from 778 MHz to 4 GHz, the effective coverage range decreases.
- A consumer cellular handset and a FirstNet handset were both assessed at 778 MHz. The FirstNet handset was shown to have a significant advantage in signal quality; however, if the "usable" range is considered equally good enough to achieve the mission, the two handsets are roughly comparable.
- The 100-W LMR/Project 25 (P25)[2] repeater provides comprehensively better coverage, especially in terrain that is hilly and contains obstructions.

One conclusion of the coverage map process is that LMR is a one-to-many communications platform, and its coverage is well suited to continue to perform in that way for the foreseeable future as a primary means of communication among public safety personnel and their agencies. PTT broadband might supplant LMR as a primary voice communications technology at some point, but the differences in the reliability of coverage mean that this is unlikely to happen in the near future as a norm of law enforcement communications practice.

Limitations

This project began before the coronavirus disease 2019 pandemic and then was delayed for several months (from April 2020 to January 2021) during the brunt of the pandemic's impact on mobility, social contact, and available time for public safety personnel to participate in the effort. The pandemic affected the conduct of interviews and surveys; a number of respondents were unable to take time away from their duties because

[1] The radio tower that provides primary coverage in the area studied is in the Verdugo Mountains, a small mountain range in Los Angeles County, with a maximum elevation of 3,127 ft. The ridgeline of the small range is demarcated as the municipal boundary between the cities of Burbank and Glendale. The range runs northwest to southeast and is bordered by I-5 to the west and I-210 on its eastern flank. According to topographic maps from the U.S. Geological Survey, the 125-ft radio tower sits at about 3,077 ft above sea level (U.S. Geological Survey, 1966). The tower is located at 34.2195412° north, 118.26863805° west.

[2] P25 was formed in 1990 in accordance with an agreement among APCO (Association of Public-Safety Communications Officials) International, the National Association of State Technology Directors, and agencies of the U.S. federal government to establish current and emerging wireless LMR communications standards that meet the requirements of the public safety community. See Cybersecurity and Infrastructure Security Agency (CISA), undated. APCO has performed a coordinative role, and has served as project director, since P25's inception (APCO International, undated b).

of the demands of deploying police officers while stay-at-home orders and social unrest from the pandemic were in full force.

The delay in completing interviews and an assessment of the state of broadband technology and its use in law enforcement, though, became an advantage to the end user because it allowed us to more fully observe the impacts of the pandemic on law enforcement communications. We were also able to assess the outcomes of police communications issues that arose with protests, riots, and similar activity in cities across the United States as a result of the in-custody killing of George Floyd in Minneapolis, Minnesota; a regional disruption to public safety broadband in the bombing in Nashville, Tennessee; the inordinately cold weather in Texas in early 2021; and other instances in which policing met novel conditions presented by both the pandemic and civil unrest. In addition, telecom providers that serve the police were able to further refine the scope of their offerings and begin deploying 5G networks in their respective broadband grids.

This report does not encompass the universe of possible providers, agency needs, or technological advances related to police broadband deployment. Although there are two national providers of law enforcement broadband services (AT&T and Verizon), other broadband providers have offerings and services that are used by some policing agencies. In addition, the development ecosystem by the National Institute of Standards and Technology (NIST) and others is moving forward at a rapid pace. It is our intent that the assessment of current and envisioned broadband systems for the police in this report will provide guidance for law enforcement leaders as they consider whether and when to upgrade or alter their LMR/LTE systems. We recognize that this analysis will not address all possible options as a practical outcome of the work.

CHAPTER THREE

Understanding Core Communications Technologies

In this chapter, we provide an overview of the core broadband communications technologies, network assets, and architectures. We also include a brief history of the transition from narrowband to broadband (1G to 4G), 5G and emerging advances, and mobile assets. In addition, we describe the emergence of the NPSBN and competing broadband vendor platforms, concluding with an overview of Next Generation 9-1-1 (NG911) and its implications for interoperable broadband. This chapter is supported by a deeper discussion of broadband technologies in Appendix A.

Understanding Core Broadband Technologies

The traditional means of mobile communication has been the police radio; increasingly, though, an officer's cell phone or similar mobile device has become as important as a means to connect to others. The capabilities of today's mobile broadband devices have opened a vista of possibilities for transmitting data, video, and real-time crime information and for serving a host of other functions. However, the sheer number of possibilities can create substantial confusion as police decisionmakers work to employ the best blend of mobile communications technologies for their officers in the field. The following discussion is intended to highlight key features and uses of each technology.

Mobile Data Platforms

Police departments have been experimenting with the use of mobile data terminals (MDTs) since 1988, when a police agency introduced notebook computers into its patrol cars to permit the use of mapping and automatic vehicle location (Monopoli, 1996). Since that time, MDTs have evolved from mere information receivers to complex, freestanding computer terminals. Interestingly, except for electronic control devices, mobile computing has been the sole principal new technology in police field operations in the past 25 years (Hollywood et al., 2016). Other aspects of an officer's equipment and uniform have been modernized, but only incrementally (Hollywood et al., 2016).

Historically, the dominant mode of communication by the police has been LMR, which uses an increasingly complex array of bandwidth to transmit voice and data communications. Increasingly, wireless broadband technologies have been adopted to transmit data, including real-time video and stored video footage from an officer's body-worn camera, or to connect law enforcement and other public safety personnel who operate on separate LMR systems but share an incident or emergency response in a jurisdiction or area that does not support one's native LMR system.

Law enforcement can use a variety of technological approaches to enhance the access and reliability of LMR coverage. These include adding technological expertise to a city or county radio system via expert resources (either employed by the agency or contracted for professional services), installing repeaters that amplify LMR coverage, and forming joint-powers agreements to create a voice, data, or voice/data entity that manages public safety communications in adjacent jurisdictions. The ubiquitous and growing presence of smartphones; their increasing speed, storage, and transmission capacities; and law enforcement's growing need to utilize added bandwidth for its purposes have created a sense of urgency among police to find answers to their voice and data needs—answers that might include both LMR and broadband solutions.

Transitioning from Narrowband to Broadband Data and Voice: 1G to 5G

Since the advent of the police radio in the early 1900s, public safety professionals have used wireless systems to receive information, broadcast their statuses, and talk with one another to coordinate their efforts. Other first responders use similar systems for medical aid, in structure fires, and to quickly deploy people and equipment to remedy the incident to which they are responding. Although the mobile broadband systems in use today are seemingly ubiquitous, their presence and functionality is a relatively recent technological development, one that has resulted in several generations that demarcate increasing complexity and utility.

It can be useful to briefly review the generations of mobile broadband to better understand how each platform built upon its predecessors and informed the broadband generations to follow.

Analog Cellular Networks: 1G

The first commercial cell phone call in the United States was placed in 1983 in Chicago by Robert Barnett, chief executive officer of Ameritech Mobile Communications (now Verizon), to Alexander Graham Bell's grandson (Mack, 2013). Barnett said, "I like to say that technology will go from the phone in the car to a phone in the briefcase to finally a phone in your pocket" ("Flashback: What We Said About Mobile Phones in 1983," 2015). Within 20 years, more than 1 billion users subscribed to mobile services (Ghosh et al., 2011). As of 2019, more than 5 billion people had mobile devices, more than half of which were smartphones (Silver, 2019). In less than 40 years, cell call capacity has grown from only a handful of people being served at one time to billions of mobile device usages each year. No longer just a means by which to make a call, mobile devices are now primarily used to access podcasts, texts, video clips, games, and music. None of this would have been possible without that first small step in 1983.

Digital Cellular Networks: 2G

The second generation of cellular networks, 2G, first emerged in Finland in 1991. This generation also saw the transition from analog to digital platforms, most notably Code Division Multiple Access (CDMA) and Global System for Mobiles (GSM), which were adopted by the major telecom providers to support their wireless technologies (Segan, 2020). 2G saw maximum data transmission speeds of about 50 kilobits per second (Kbps), a 12-fold increase from 1G (Verizon, 2019). Although 2G gave users smaller devices, better call quality, and more-secure connections, it gave way to a third generation of mobile wireless in 1998.

Mobile Broadband: 3G

The third generation, 3G, emerged as a result of work in the early 1990s, when the International Telecommunications Union (ITU) sought to create global interoperability at scale and at a lower cost through 3G systems in the 2,000-MHz range (known as IMT-2000) (Ghosh et al., 2011). In 1998, the official standardization process transitioned to a collaborative known as 3GPP (the 3rd Generation Partnership Project; see 3GPP, undated), which is the de facto governing body for GSM, which is used by most of the world outside of the United States (Segan, 2020). 3GPP united seven telecommunications standards development organizations to facilitate a stable environment to define 3GPP technologies.

As fixed-line broadband also grew rapidly, however, mobile broadband companies recognized the need to develop a system commensurate with cable and DSL "hardwired" connections that could support the growth of internet protocol (IP) traffic. In 2005, 3GPP began work to develop LTE and Systems Architecture Evolution standards. This created standards for a fourth generation of mobile communications (Hill, Chandler, and Beaton, 2021).

4G LTE

Around 2005, 3GPP's radio access network began work on the LTE project. The introduction of Apple's iPhone in 2007 accelerated mobile subscriptions, which rose from two per 100 people in 1990 to 92 per 100 people in 2010 (Qualcomm, 2014). As 4G LTE was introduced, it leveraged the dependability of data-optimized 3G broadband (which enabled voice services and global roaming) with faster speeds and higher data capacity abilities (Qualcomm, 2014).

Although many people with smartphones might believe their devices are "4G" technology, a few will notice the abbreviation "LTE" following the 4G reference. This is because LTE is the project name given to the high-performance interface for cellular communications that differentiates it as more than "3G"; however, in technical terms, LTE is not yet a 4G-compliant technology.

True 4G and LTE-Advanced (LTE-A) improve upload and download speeds tenfold as compared with LTE and significantly reduce latency to improve lag times, which enhances streaming live video and makes for clearer voice and video calls. It is important to remember that a 4G-LTE, LTE-A, or 4G device will work only as well as the network supporting it. Not all 4G networks are the same, and the ultimate performance of a mobile device will depend on the underlying systems and technologies, the location from which transmissions are made and received, and the type and capabilities of the device.

5G

In 2017, 3GPP approved the specifications for the next generation of mobile broadband, 5G (3GPP, 2017). 5G will provide end users with higher speeds and lower latency, which is the lag time between communications and data from device to device (3GPP, 2017). It should also facilitate a broadband system that allows transitions between different Wi-Fi networks and between cellular networks and Wi-Fi, allowing more devices to be connected and much higher download speeds (Brown, 2020). As 4G is fully deployed, public safety end users have already begun to see early versions of 5G devices and technologies enter the market. As 5G standards are emerging from the development process into the first generation of user access in the United States, there are issues for public safety that are critical to consider. Among these issues are voice-data integration standards; P25 public safety standards; the management of unmanned aerial systems (UAS); and the Nationwide Public Safety Network's deployment of 5G-compatible devices for the NPSBN.

FirstNet and the NPSBN

The FirstNet NPSBN is intended to help "law enforcement, firefighters and EMS save lives and protect communities across the United States" in a "reliable, secure broadband network dedicated to public safety" (FirstNet.gov, undated). Although the original intent of FirstNet's mission was to create a nationwide cellular system for first responders alone, the cost of such a system was unfeasible. In light of this, FirstNet opted to allow existing cellular vendors to build the network (Griffith, 2017). In March 2017, AT&T was awarded the contract in return for its commitment to spend $40 billion over the next 25 years to create and maintain FirstNet and to connect it to AT&T's $180 billion telecommunications network, which reaches 99.6 percent of the U.S. population (Sambar, 2017).

Under the agreement with FirstNet, AT&T would give first responders usage priority to preempt access to the network by other cellular users. Although the 9/11 Commission envisioned that a public safety–specific spectrum would be allocated, the chosen approach in 2017 was to allow law enforcement to use all of the commercially allocated spectrum on an as-needed priority basis (Griffith, 2017). The FirstNet LTE mobile network, though, is "not a nirvana" and is not meant to replace the radio systems in use by police and fire departments (Jackman, 2017). Some skepticism in law enforcement exists, in part due to the cost to equip officers with department-supplied mobile phones and the subscription cost once an agency migrates to the FirstNet platform (Jackman, 2017). In spite of these concerns, all 50 states, five U.S. territories, and the District of Columbia opted into a commitment by FirstNet to build, operate, and maintain the network by early 2018 (FirstNet.gov, undated).

On March 7, 2018, FirstNet announced its nationwide launch of the AT&T build-out of the PSBN (FirstNet.gov, undated). Its press release emphasized that only AT&T can implement the Band 14 public safety spectrum to "give first responders access to its unique attributes" (FirstNet.gov, undated). Once implemented, the network will be the foundation for

- end-to-end encryption, with advanced physical and logical security protocols to keep all network traffic protected
- around-the-clock security monitoring by a dedicated security operations center
- superior reliability with a 99.9-percent end-to-end service availability objective
- local control for differing levels of priority so that incident commanders and eligible first responders can boost priority levels to support situational responses
- mission-critical next-generation public safety capabilities currently under development, including Mission-Critical PTT (MCPTT) and enhanced location-based services.

Although the FirstNet build-out is progressing according to the contracted schedules, significant issues remain to be resolved at the local level. About 70 percent of police agencies do not equip their officers with phones (Jackman, 2017). FirstNet will provide SIM cards to enable existing smartphones to access its network, but those phones will need specific apps to optimize the reception and security of photos, videos, and related wireless data. Although the first approved mobile apps were not available until after 2017 because of the relatively small user population of fewer than 4 million people (Jackman, 2017), the FirstNet.com catalog now lists 100 approved apps for FirstNet's mobile devices (FirstNet, 2019). At the same time, FirstNet's build-out is ahead of schedule, having passed 95-percent nationwide coverage in its first four years. As of December 2021, FirstNet had more than 19,500 public safety organizations using more than 3 million connections nationally (Jackson, 2022).

It should be noted that there might be necessary additional costs related to communications hardware, such as mobile routers and modems, to support any future system. Edson (2019) notes that some routers and modems are not compatible with FirstNet, so agencies might have to remove old equipment and replace it with FirstNet-compatible devices. The "Connected Cop" network pioneered by the Los Angeles Regional Interoperable Communications System (LA-RICS) is one promising approach that eliminates the mobile data computer and relies on the smartphone or tablet to interface with other persons and agencies in the communications network. Agencies choosing this approach should consider the signal strength of the mobile device when it is distant from the vehicle's router or modem (e.g., if an officer moves into an area where there is no cell reception) and device battery usage over time when the device is in the unit transferring data (Edson, 2019).[1]

FirstNet services come with an array of mobile base stations from which users may request for preplanned or emergency purposes. FirstNet also deploys Cells on Wheels (COWs) and Cells on Light Trucks (COLTs) for emergency support from prestaged locations around the United States. Other cell phone providers own

[1] LA-RICS was an early builder of the NPSBN; it was formed in 2009 as a joint-powers authority to build and operate a public safety broadband data network. See Edson, 2019, for more information about the Connected Cop network and other LA-RICS advancements.

and deploy COWs for temporary use for their customers (Banse, 2017). FirstNet defines its COLTs as Satellite COLTs (SatCOLTs). COWs generally denote larger, more robust systems that can remain at a site for extended periods, as needed.

FirstNet stages its more than 70 COWs and COLTs in 40 locations across the United States, and its National Disaster Response Team maintains its mobile fleet in four "strategically placed" warehouses domestically (plus a fifth to support overseas markets) to enable a 14-hour delivery window to an emergency request for support. AT&T's capabilities include three "Flying COWs" (for "Cells on Wings") and "FirstNet One," a deployable blimp (Sambar, 2019). FirstNet's COWs also can deploy an all-weather "Flying COW drone" to extend the range of the COW ("AT&T's New Flying COW Drone to Be All-Weather Disaster Insurance," 2018). FirstNet's first such use of these dedicated resources was of a SatCOLT, sent to Chino, California, to keep officers connected during a Fourth of July celebration in 2018 (Douglas, 2018).

Scheduled Termination of FirstNet's Authority in 2027

There is a significant issue that will necessitate congressional action in the near future to ensure the continuity of the NPSBN. The legislation that created the NPSBN in 2012 terminates FirstNet's authority in 2027, and it does not identify how the NPSBN should be managed after that. The U.S. Government Accountability Office (GAO) identified four key statutory requirements and contract responsibilities performed by FirstNet upon which Congress should act prior to the expiration of the 2012 legislation (GAO, 2022). The report lists three options to address FirstNet's termination of authority in 2027 if Congress elects to reauthorize FirstNet's authority: "(1) keep it within the National Telecommunications and Information Administration (NTIA); (2) place it within another federal agency; or (3) establish it as a separate federal organizational entity" (GAO, 2022, pp. 2–3). GAO notes that FirstNet officials say that separating FirstNet "from another executive branch agency would enable it to exercise its authorities without undue constraints from a federal agency" (p. 3). The report further notes that "disadvantages include the need to establish mission-support services (e.g., financial and legal support) and the loss of available oversight mechanisms, such as from the Department of Commerce's Inspector General" (p. 3).

On February 18, 2022, H.R. 6768 (117th Congress, 2021–2022) was introduced to delete the termination clause of the 2012 legislation (U.S. House of Representatives, 2022), but it does not (yet) include direction regarding the options listed by GAO. As of this writing, it is unknown whether this bill or companion legislation will provide specifics of the management of FirstNet.

Alternative Public Safety Platforms and Services

Although AT&T was the lone qualified respondent to the request for proposal (RFP) issued to contract for the construction of FirstNet,[2] that does not mean that other broadband providers abandoned the public safety mobile broadband market. One competitor offers services and capabilities that it would assert are comparable with those of FirstNet; another broadband provider has moved into the first responder market segment; and others might also provide preferential services for law enforcement agencies on a local or regional basis that are attractive to a chief or sheriff as they work to limit costs for this capability.

Verizon is the most prominent broadband provider to challenge AT&T's build-out of FirstNet, matching many of AT&T's service and technology offerings as they are announced. For example, even as the federal government was working with AT&T to launch FirstNet, in August 2017, Verizon announced its intention to

[2] There were two other bidders for the RFP that were excluded for not being in the "competitive range," which includes only the "most highly rated" proposals (Jackson, 2017). One bidder filed a lawsuit that was resolved in AT&T's favor in March 2017, clearing the path for FirstNet to sign a contract with AT&T to provide services.

build a dedicated network core for public safety and "invest in new mission-critical 4G LTE voice communications to complement existing services such as Push-to-Talk Plus" (Verizon, 2017).

In March 2018, AT&T launched and delivered the FirstNet core to the First Responder Network Authority to provide "end-to-end encryption," "around the clock security monitoring," "superior reliability and availability," and support for a host of mission-critical functions and capabilities (Bratcher, 2018). That same month, Verizon unveiled its public safety private core and stated that public safety agencies nationally would receive preemption and mobile broadband priority services (Verizon, 2018).

As AT&T works to complete the NPSBN, new capabilities and services are announced as they occur. As happened with the timing of the FirstNet core announcement, Verizon also publicizes similar capabilities. On April 1, 2021, AT&T announced three "major milestones" for FirstNet: a first responder–centric approach to 5G; comprehensive tower-to-core network encryption; and the FirstNet Health and Wellness Coalition to better support responders holistically (FirstNet, 2021). On March 4, 2021, Verizon announced the launch of Verizon Frontline to introduce an "advanced network and technology that has been built for first responders" (Verizon, 2021). Verizon's webpage dedicated to its public safety network and technology is now named VerizonFrontline and includes a section discussing 5G services for its public safety platform (Verizon, undated). Frontline is more of a means to brand Verizon's public safety offerings than a new network or technological approach (Engebretson, 2021). Neither AT&T nor Verizon publicly discusses the specific capabilities that its 5G networks might have now or in the future, since that information would be considered intellectual property.

In January 2021, Verizon called for "true interoperability" between its systems and the NPSBN (Jackson, 2021a). The company's call for interoperability is consistent with comments that it submitted to the U.S. Department of Commerce on November 9, 2012 (Verizon, 2012). At that time, Verizon recommended a "diverse nationwide network" for FirstNet as a public-private partnership instead of a standalone public safety broadband system (Verizon, 2012, p. 3). However, an editorial by a past president of APCO International[3] noted that Verizon had previously objected to sharing core network components (i.e., the IP Multimedia System and Evolved Packet Core) in a 2012 statement to the U.S. Department of Commerce and that the company's call for true interoperability was not consistent with its previous stance (Mirgon, 2019). The FirstNet Authority asserts that claims of special interoperability needs are not true, since the NPSBN is a 3GPP standards-based platform whose solutions "not only provide interoperability, but also foster creative innovation for Mission Critical services [and] provide economies of scale" (Parkinson, 2020).

To further complicate matters, subsequent to its merger with Sprint, T-Mobile entered the public safety broadband market in May 2020. T-Mobile pledged a $7.7 billion investment over ten years and free unlimited mobile and 5G services to first responder agencies nationally (Alleven, 2020). A GAO ruling in April 2020, however, determined that T-Mobile could not meet public safety requirements as established in a request for quotations for a federal agency (GAO, 2020). T-Mobile's merger with Sprint did give the company added bandwidth in the low- and mid-band frequencies, differentiating it from its competitors in this market.

Although the presence of market competitors to FirstNet can confuse the end user, FirstNet's efforts to gain or retain a customer base can work to the benefit of the public safety community by encouraging AT&T to remain diligent in its work to sustain a competitive advantage over Verizon or others vying for the same market. In spite of the competition, FirstNet subscriptions continue to grow, with about 15,000 agencies and 1.9 million connections achieved by the end of 2020 (Jackson, 2021b). Subscribers include the Federal Bureau of Investigation's (FBI's) announcement in December 2020 of a five-year, $92 million contract to move away from Verizon to FirstNet, the largest agreement by a law enforcement or first responder agency in the United

[3] APCO International, founded in 1935, is made up of more than 35,000 members who manage, operate, and build public safety communications systems for first responder agencies.

States at the time ("FBI Switches Remaining Operations from Verizon to FirstNet," 2020). The FirstNet Authority Board also approved $218 million in July 2020 for FirstNet communication network upgrades, including investment in 5G capabilities (Descant, 2020). According to its 2021 annual report, FirstNet had launched Band 14 coverage in 700 markets and reached 80 percent of the nationwide coverage by the end of fiscal year 2020 (Hill, 2021).

AT&T has a persuasive advantage in bandwidth allocation, since Band 14 is dedicated solely to public safety needs. Verizon would counter that Band 13 is a commercial band, but that they offer similar mission-critical prioritization, prioritization and preemption, and public safety–dedicated services. AT&T has direct oversight by the FirstNet Authority to ensure that it complies with the mandates of the NPSBN contract, although Verizon and T-Mobile might assert that their coverage is better, more reliable, and not constrained by a government contract. As a contractor to the FirstNet Authority, AT&T also specifies support capabilities more precisely. For example, AT&T identifies the number of COLTs, COWs, and related support equipment, while Verizon does not provide specific numbers of COWs, COLTs, or Generators on a Truck (GOATs) ready for deployment by public safety agencies but notes that they can be "prepositioned when you can plan and are positioned geographically to respond when you cannot" (Kozlowski, 2020). In 2018, Verizon noted that it has one disaster equipment storage location near Kansas City, Missouri, the only such facility nationally. In it, Verizon stores its complement of COWs, COLTs, GOATs, and Cell Repeaters on Wheels (CROWs) to await deployment anywhere in the United States (Johnson, 2018).

As a counter to the FirstNet Authority, Verizon has created a Public Safety Advisory Council to interact with first responder communities as they develop their priorities and strategies for the future ("Verizon Launches Public Safety Advisory Council Event Series," 2020). Verizon's advisory board is not a formal oversight entity like the FirstNet Authority Board, but rather a part of Verizon's corporate effort to refine and develop its public safety broadband services for the future.

As FirstNet's applications grow, and as interoperable capabilities are solidified among the carriers and FirstNet, the primary questions will remain for end users—who provides better coverage, who can provide public safety–grade equipment and technologies, and who can ensure continuity of broadband services no matter the circumstance?

NG911

Although not specific to broadband systems, the 911 PSAP/emergency communications center (ECC) function and the current move to adopt NG911 standards are important to discuss—not only because the same ECC will handle emergency calls for the police via 911, but also because they are the locus of control for LMR and LTE transmissions and future interoperability.

In 1968, the phone number 911 was established as the universal emergency number for persons needing to contact first responder agencies (National 911 Program, undated). 911 PSAPs, though, were built using analog technologies and have not been modernized as public communication systems have migrated to digital platforms. According to APCO, in existing 911 networks, the public can make primarily voice and teletype calls, with only data that includes automatic number identification, subscriber name, and automatic location identification if it is available (APCO International, undated a). Now that more than 80 percent of the public uses mobile devices to send and receive data, videos, photos, and other forms of communication, existing 911 technologies cannot access that information.

A large-scale project to upgrade 911 systems nationally seeks to move those systems to digital communication platforms to allow ECCs to receive and share digital information from officers and the public, including photos, text, video, audio, and closed-circuit television footage. Dispatch centers on NG911 platforms will be able to receive critical data and then push those data to officers in the field (National 911 Program, undated). As envisioned (and currently being used for states that have completed their NG911 systems), NG911 will

- enhance location accuracy because of NG911-enabled mapping technology and because NG911's technology will enable 911 calls to determine the appropriate PSAP automatically, allowing ECC personnel to specifically locate callers faster and more accurately
- provide better, quicker access to video, photo, and data media sent to law enforcement by the public so that victims and witnesses can transmit suspect images or other critical information
- have redundancy and multi-ECC interoperability in times of need by rerouting calls or other data to alternate PSAPs
- provide more-complete situational awareness for officers responding to emergency calls or on the scene at incidents, through better data-sharing, and provide real-time access to sensors, cameras, or witness data during emergencies (National 911 Program, undated).

NG911, unlike FirstNet, is being implemented by states, regions, and municipalities, and stages of completion vary widely. Some states have adopted plans that include governance, systems standardization, and funding mechanisms, and some have completed their NG911 transitions. FirstNet, however, will be enhanced if it is in use in agencies that have NG911 ECC platforms. FirstNet applications can take advantage of both FirstNet and NG911 networks, enhancing interoperability and the seamless transfer of data between the two systems.

Satellite Communications

Satellite communications (SATCOM) use artificial satellites in earth's orbit to relay signals from one terrestrial location to another. The advantage of this approach is that one satellite can provide coverage to areas without installed infrastructure and thus extend services to remote rural locations without the need for fixed cellular infrastructure. Artificial satellites are also unaffected by natural or manmade distracters that might disable existing cellular infrastructure and thus provides a backup communications pathway. We previously mentioned COLTS and COWS that can provide emergency cellular infrastructure in areas without coverage. These include a cellular base station that provides service to subscribers and then connects back into the core service provider network either through the terrestrial fiber network or, if the fiber network is not available, through a satellite connection. Those SATCOM terminals are generally larger and need to be carried by a vehicle or platform.

Small, handheld SATCOM devices exist that can provide connectivity without the need for fixed infrastructure. Iridium satellite phones are an example of such devices; they provide voice and low-data-rate services across the globe (Iridium, undated). These are simpler devices and do not include the smartphone capabilities typical of most modern cell phones. The services are also considerably more expensive, and service providers typically charge by the minute of each call and by each megabyte (MB) of data sent and received; therefore, these devices are used sparingly and only by organizations with considerable resources. There are some devices on the market (such as the Thuraya X5-Touch satellite smartphone) that have smartphone functionality and are designed to be dual use over both cellular and SATCOM networks, but, again, these suffer from higher costs to purchase and operate. There are vehicular systems that provide automatic switchover to a high-bandwidth SATCOM connection when cellular is not available that are particularly useful in areas with spotty coverage, such as remote rural and border areas (Stevenson, 2018).

Gateway and Interoperability Technologies

Communications often need to traverse multiple types of communications networks between LMR systems and broadband networks. There are three major technical approaches to provide connectivity between LMR and broadband. These are shown in Figure 3.1.

Internet Protocol Solution

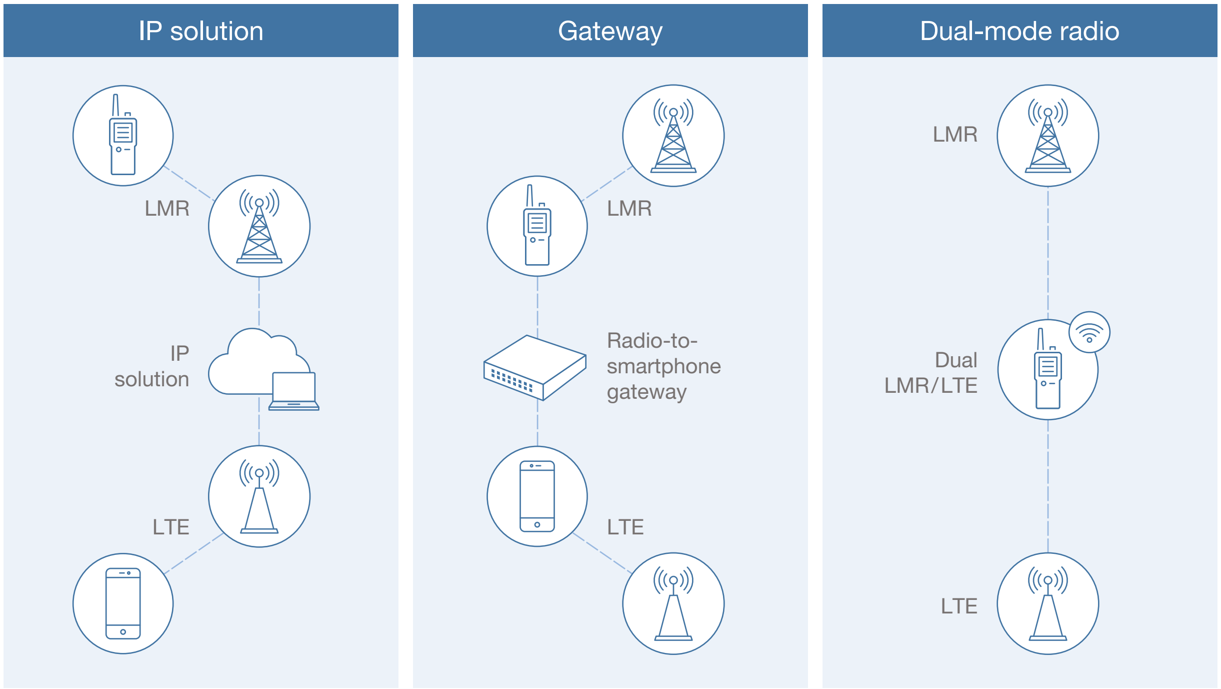
The most comprehensive solution to achieve interoperability between two or more LMR and LTE networks is an IP solution, in which LMR communications go across a base tower, get digitized and translated and go across an internet-based network, and then get translated and broadcast out over an LTE network (see, for example, Paulson and Schwengler, 2013).

The advantage of this approach is that it allows complexity and scale: It permits managed integration over a potentially large number of LMR and LTE groups. The disadvantage is also the complexity and scale; the solution requires a substantial commitment in cost and time to set up and maintain. Furthermore, IP solutions might introduce their own interoperability problems if they work with one vendor's LMR networks but not another's.

Gateway

A gateway is a dedicated device to which an LMR handset from one talk group is connected on one side and an LTE broadband device from a second talk group is connected on the other; it mediates communication across both devices and, hence, across both groups. The advantage of this approach is its simplicity: The cost per gateway and the amount of time to set up a bridge across two talk groups are both small. The disadvantage, similarly, is also its simplicity: One device bridges just two talk groups across two colocated devices.

FIGURE 3.1
Technical Approaches to Connect LMR and Broadband Networks



This solution also takes two devices (one LMR handset and one LTE device) out of circulation, as they have to be plugged into the gateway.

Dual-Mode Radio

With a dual-mode radio, one LTE handset doubles as both an LMR handset and an LMR-to-LTE gateway between an LMR talk group and an LTE talk group. In addition to not needing a separate gateway device, this approach typically allows the sharing of some data between LMR and LTE parties besides voice communications, which are typically tracking data. Its advantages are similar to those of the dedicated gateway; it is easy to set up and comparatively inexpensive per pair of talk groups bridged. Its disadvantages are also similar—one device bridges only two colocated talk groups—and there is the added expense of an LMR device that is capable of serving as a gateway.

Summary of LMR-to-LTE Solutions

An IP-based solution is intended for agencies that need large-scale bridging of talk groups across LMR networks and LTE mobile networks. The other two solutions—gateway and dual-mode radio—are intended primarily to bridge individual pairs of groups and will be more applicable to agencies that have only one or a few groups to bridge across LMR and LTE networks.

Putting the Pieces Together: Communications Architectures

Variety of Potential Devices on Broadband

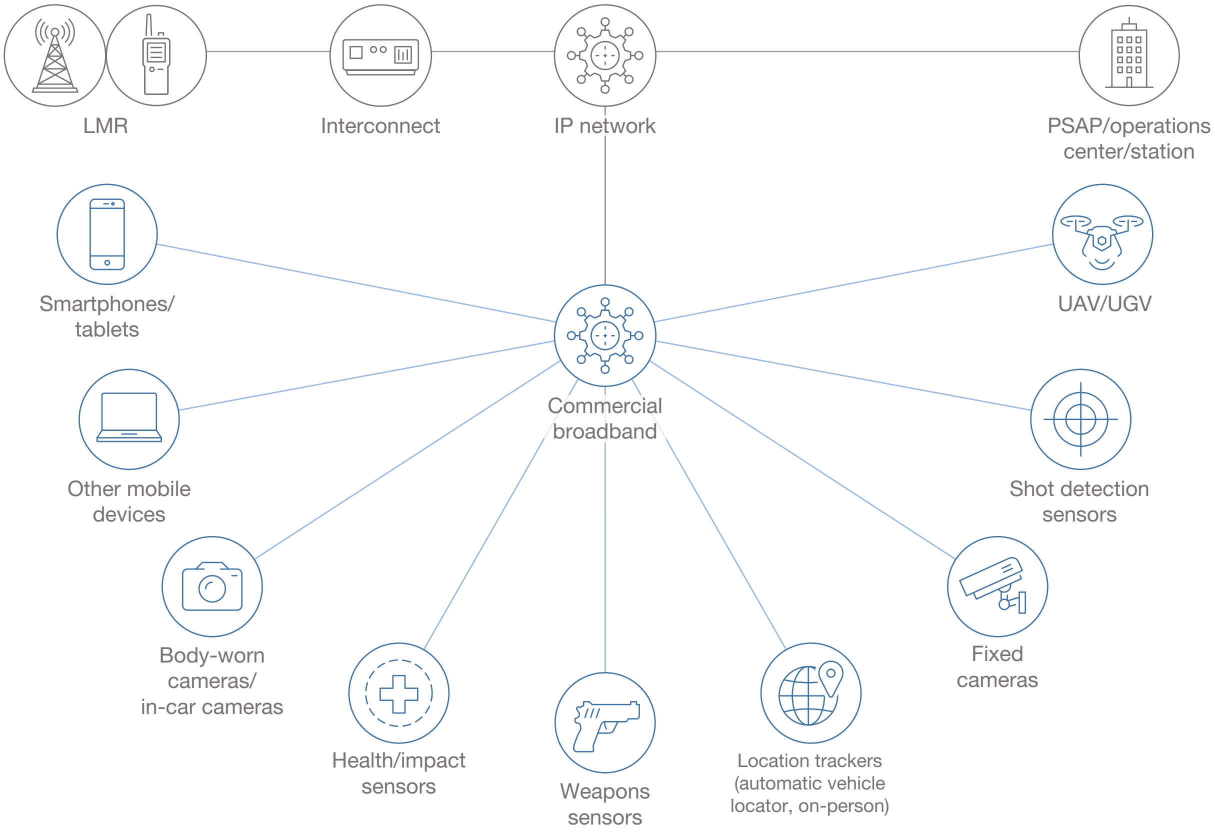
The variety of potential devices that can be brought onto broadband law enforcement networks is wide, as shown in Figure 3.2. The core devices are likely to be officers' smartphones or tablets, along with other mobile terminals and similar mobile devices (e.g., in-car mobile data computers). However, there are also various potential wireless-enabled sensors, such as

- streaming video cameras of all formats, including fixed and mobile surveillance cameras; streaming of in-car and body-worn cameras is expected to increase over time
- officer life-safety sensors, including sensors measuring the officer's health (e.g., warning signs of a potential heart attack), alerting if the officer has just been involved in a high-impact event, or alerting if the officer has pulled their weapon
- location trackers for police vehicles and on-person trackers
- networks of shot-detection sensors
- video and control feeds from small autonomous vehicles, including UAVs and UGVs.

All of the above will require mobile connectivity services, just like smartphones and tablets, potentially including mobile service subscriptions.

In terms of bandwidth consumption, streaming video will consume large amounts of data. Specific amounts will vary depending on reception and the specific video compression algorithms being used, but estimates are as follows:

FIGURE 3.2
Variety of Devices on Law Enforcement Broadband Networks



- standard definition (480p[4]) video will consume around 300 MB, or 0.3 gigabytes (GB), per hour
- high-definition (which will range from 720p to 1,080p to 2Kp, depending on reception quality) video will consume from 0.9 GB (for 720p) to 1.5 GB (for 1,080p) to 3 GB (for 2Kp) per hour
- now-emerging ultra-high-definition video (4Kp) consumes around 7.5 GB per hour (Hildenbrand, 2020).

In comparing these data consumption rates with typical monthly data limits on mobile plans (typically 2, 5, or 10 GB per month), one can see how streaming video can exhaust mobile broadband data limits quickly.

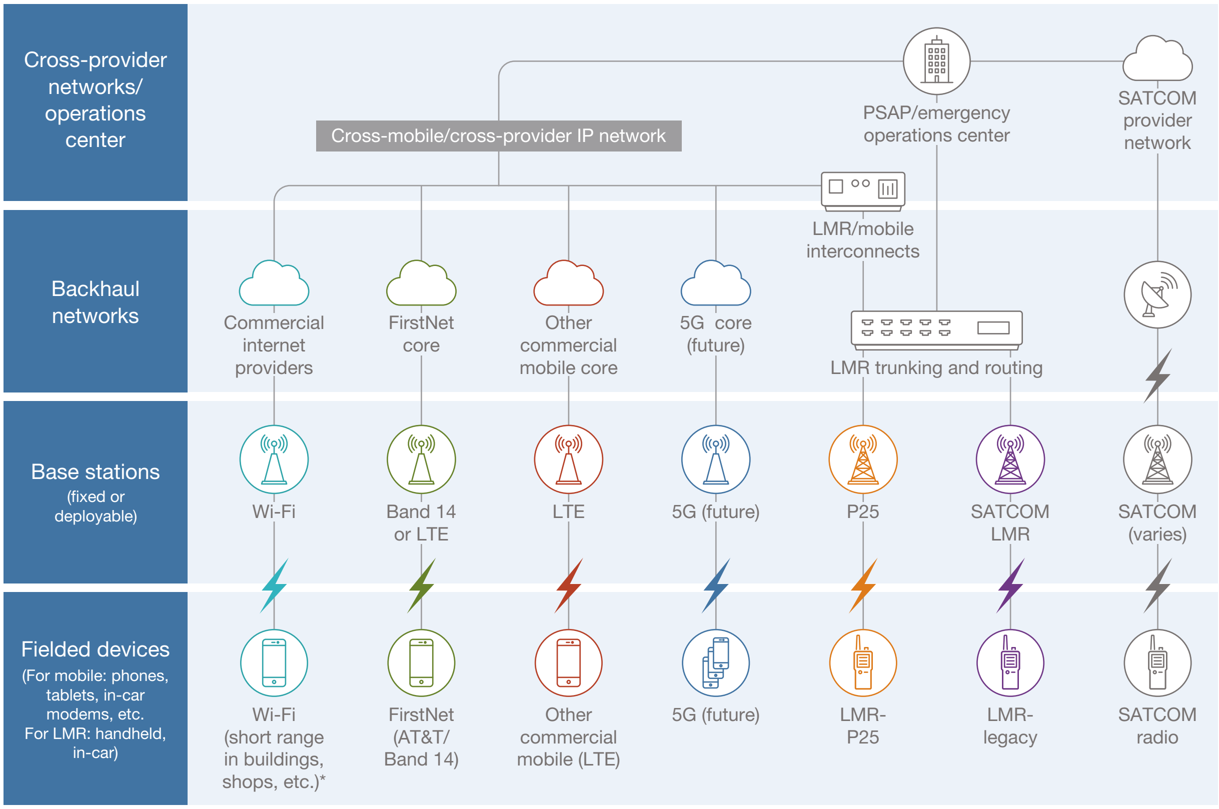
Practical Architectures

Figure 3.3 shows more detail of how a network needing to provide communications across a variety of legacy and new systems might be structured. The bottom row of the figure contains the full range of types of wireless devices that might be on an agency's network, including broadband and legacy devices. (For the sake of simplicity, these are all shown as "devices," not separated by whether they are, e.g., smartphones, tablets, handheld radios, or sensors.) On the left side of the figure are the broadband devices that will be primarily

[4] *480p, 720p* is a measure of screen resolution.

FIGURE 3.3

A Mixed Law Enforcement Communications Network


Cross-provider networks/ operations center
Backhaul networks
Base stations (fixed or deployable)
Fielded devices (For mobile: phones, tablets, in-car modems, etc. For LMR: handheld, in-car)
Cross-mobile/cross-provider IP network
PSAP/emergency operations center
SATCOM provider network
LMR/mobile interconnects
Commercial internet providers
FirstNet core
Other commercial mobile core
5G core (future)
LMR trunking and routing
Wi-Fi
Band 14 or LTE
LTE
5G (future)
P25
SATCOM LMR
SATCOM (varies)
Wi-Fi (short range in buildings, shops, etc.)*
FirstNet (AT&T/ Band 14)
Other commercial mobile (LTE)
5G (future)
LMR-P25
LMR-legacy
SATCOM radio

*The same smart device can use Wi-Fi and cellular (LTE, etc.).

on commercial broadband networks, including FirstNet, other commercial LTE, and 5G (in the future). On the right side are legacy radios, including P25-compliant LMRs and older or noncompliant LMRs.

On the far right of the figure are SATCOM radios, intended to provide service when personnel are out of range of any line-of-sight–based communications service. (Not shown, but also relevant, are either LTE or LMR devices that communicate within line of sight to a SATCOM vehicle, which then communicates with a communications satellite.)

All of these various types of devices, in turn, communicate with some form of base station, whether commercial towers or access points (for broadband), various LMR towers, or communications satellites. These then transmit through the various services' backhaul networks.

Communications need to be translated, integrated, and retransmitted back out to the field to permit interoperability across devices. As discussed previously, this is increasingly being done via internet (or IP-based) solutions. The communications then feed into the agencies' local PSAPs or emergency operations centers, or both. It is from these centers that public safety telecommunicators (e.g., 911 dispatchers), as well as agency commanders, can communicate with units in the field.

Conclusion

In this chapter, we examined the core broadband technologies and their application to law enforcement and emergency responders. It is important to note that there are a wide variety of device options and service providers, and there are many different systems that make up a law enforcement and emergency responder network. The network architecture can include a variety of cellular providers, backhaul providers, LMR, and gateways and interconnect points to bring all of these different systems together. While it is important to understand the technology and how it comes together to form a network architecture, it is equally important to understand how this infrastructure and set of end-user devices should be managed. This is the topic of the next chapter.

CHAPTER FOUR

Governance and Operational Requirements

> "You can have all the technology you want but you will not achieve true interoperability if you do not have the cooperation and the collaboration that comes with the governance structure that ensures everyone is working together, making joint decisions, spending funds with others in mind."
> —SAFECOM Executive Committee Chair Marilyn J. Praisner (SAFECOM and National Council of Statewide Interoperability Coordinators, 2018, p. iv)

While understanding the variety of available technologies is one key step in building a broadband communications capability, first responder networks also require a governance structure to maintain and operate them effectively and a set of policies to codify this structure. We thus begin this chapter by describing the various governing bodies involved in police communications and some policies related to broadband.

It is important to understand both how these networks can be used in practice and how they operate in the field under various conditions and while using different types of communications infrastructure, software, and services. In this chapter, we discuss five use cases: routine policing, major criminal response, mass attack response, major event security, and disaster response.

Governing Bodies for Police Communications

First responder communications networks are the product of the civil authorities that design, deploy, and maintain any given system. As a result, developing interoperable systems requires regional governance with the authority to coordinate strategy across jurisdictions and marshal resources to initiate and maintain operations and with the proper structure to oversee successful implementation. Designing and maintaining effective communications governance is "one of the greatest challenges that face emergency communications officials" (SAFECOM, 2020). Any governance structure faces the complex task of creating a reliable communications system while balancing the desires of its component member agencies. There is wide diversity in the structure and sophistication of governing bodies for first responder communications, depending on the given region; the values of local leaders; the available resources; and the degree of cooperation among local, regional, and state entities.

Key Components of Governance

The importance of governance has been emphasized since the goal of national interoperability was established. Much of the literature and many of the resources for communications governance have been produced through agencies within the U.S. Department of Homeland Security, specifically CISA. The first goal of CISA's 2019 *National Emergency Communications Plan* is to "develop and maintain effective . . . governance and leadership" (CISA, 2019, p. 11). CISA also manages SAFECOM, the primary national stakeholder organization that provides direct guidance and best practices, such as in its 2018 report, *Emergency Com-*

munications Governance Guide for State, Local, Tribal, and Territorial Officials (SAFECOM and National Council of Statewide Interoperability Coordinators, 2018). Emergency communications systems cannot function without governance that establishes clear lines of authority, establishes priorities for investment, and ensures functional operation when necessary. As one of our interview subjects reported, governance is "one of the keys for transitioning to broadband" given the complex coordination among the various stakeholders involved.[1]

Despite the variety of governance models, there are critical characteristics that all governance bodies must have to ensure the effective deployment and operation of communications systems. According to SAFECOM and the National Council of Statewide Interoperability Coordinators (2018), these characteristics include possessing documented authority related to official plans and resolutions, gathering active and accountable membership, meeting frequently and consistently, and planning often for emerging scenarios. Simply stated, governance bodies must have the authority to make official plans for their jurisdictions and the capacity to carry out those plans with the support of their members. While the specific activities used to achieve these responsibilities vary with the context and level of government, the purpose of defining and implementing strategic plans remains the same.

Communications Technology and Sustainment

While different levels of communications governance deal with parts of the communications ecosystem, they all operate in two key functional areas: communications technology and operational sustainment (SAFECOM and National Council of Statewide Interoperability Coordinators, 2018). Whether responsible for LMR, broadband, or emergency alert systems, governance bodies must ensure that the appropriate technology is being invested in, utilized, and maintained in preparation for all scenarios. For some regions, a single governance body oversees all technology verticals, but, in many instances, specific technology functions are overseen by their own authorities. LMR, broadband, or 911 can all be operated by their own governance authorities, depending on legacy governance systems and the desires of local leaders. No single governance design is uniformly more appropriate, as any combination of authorities can effectively plan and coordinate their activities to meet their region's needs. Of course, technology alone does not create an effective communications system, and operational sustainment includes the systems and practices to ensure that the technology functions as needed. These activities include resource coordination, training, and exercises for use in emergency scenarios. Through strategic plans, funding, and formal agreements between partners, governance ensures that the emergency communication system has the technology and the operations to properly function.

Cooperation and Coordination

Facilitating the continued push toward increased emergency communications interoperability has required a greater degree of cooperation between governance bodies. At the state and federal levels, this has included CISA's 2010 establishment of the National Council of Statewide Interoperability Coordinators (NCSWIC) for the coordinators "from the 56 states and territories" (CISA, 2020). The council maintains formal governance bodies, establishes communications plans, and coordinates the dissemination of training and information for its members.

[1] Interview with representative from an agency contacted for end-user insights.

State, Local, Tribal, and Territorial Governance

At lower levels of government, communications governance and efforts to promote interoperability are far more varied. SAFECOM and National Council of Statewide Interoperability Coordinators (2018) describes an *interoperability continuum* as including the various stages of governance coordination between state, local, tribal, and territorial entities. At the least coordinated end of the continuum are individual agencies working together. The next step toward coordination is informal agency coordination, which is followed by regular collaboration between key staff. The most coordinated end of the spectrum is a "Regional Committee Working Within a Statewide Communications Interoperability Plan Framework" (SAFECOM, 2021, p. 3). SAFECOM's use of a continuum rather than discrete phases reflects how coordination between governance bodies is not always the result of a linear or straightforward process. Trust-building partnerships between agencies can include informal working groups, committees, or participation in shared training exercises. Subsequent steps might involve formal planning and investment to allow interoperability of individual systems and the accompanying formal memorandum of understanding and governance structures to manage shared assets or investments. For such systems as prioritized broadband, this formal governance also includes the operation emergency response. As one regional coordinator whom we interviewed stated, "You need to have a governance scheme to decide who gets what priority and when . . . and this governance needs to be local by region."[2]

For many agencies, interoperability exists in varying degrees through different communications media depending on previous coordination efforts. For example, while many agencies operate their own local radios, Orange County, California, has operated a countywide interoperable LMR service overseen by the county sheriff's department since 1973. Managing, maintaining, and upgrading this radio system has required formal, regional governance. While Orange County's governance is well defined for LMR, each agency is still left to oversee other communications operations, such as the use of wireless broadband. In contrast, neighboring Los Angeles County is still in the process of enacting countywide radio integration.

Any regional governance must account for the specific needs, resources, and inherited legacy systems of agencies participating in that governance process. Determining the appropriate governance system and how to operate it depends on the technology, funding mechanisms, and operational systems required for a region's communications needs. Emergency communications leaders should recognize the importance of effective governance, regardless of its specific design, for ensuring that their jurisdictions are protected in any disaster. Table 4.1 summarizes the characteristics and activities of broadband governance structures.

Policies for Broadband

The specific policies for any given agency's broadband usage vary, since many agencies continue to determine the extent to which broadband services can reliably meet their needs. Such factors as budget availability, broadband coverage penetration, and personnel affinity for novel technology can all play roles in an agency's decision to invest in broadband. Although the use cases that follow demonstrate the variety of broadband-connected devices that have the potential to facilitate an agency's operations, the preliminary decision facing many of the agencies whose representatives we interviewed revolved around the extent of mobile device usage. While most agencies relied on mobile devices in some form, even if for informal communication on personal devices, there was no universal solution.

One significant factor in officer broadband usage is a desire to ensure software compliance with reporting standards. For decades, agencies have faced the decision of reporting their crime data in the National

[2] Interview with representative from an agency contacted for end-user insights.

TABLE 4.1
Characteristics and Activities of Governance Structures

Characteristic	Activities
Establish a formal and documented authority for agencies to act	• Establish formally through executive order, statute, or resolution. • Create a charter and strategic plan. • Maintain an open and transparent forum to promote greater partner buy-in.
Gather an active, balanced, and accountable membership	• Determine membership size and representation to maintain inclusiveness while permitting quorum to be met regularly. • Align needs and priorities across various members who have a role in, or are affected by, communications-related initiatives. • Document roles, responsibilities, and membership requirements and routinely assess whether stated roles, responsibilities, and membership requirements are met. • Determine how member attrition will be managed. • Manage internal, jurisdictional, and regional differences. • Ensure that member participation is sanctioned and supported by the agency or entity the member represents.
Meet frequently and consistently	• Provide multiple means to participate in meetings (e.g., in person, videoconference, webinar, teleconference) while advancing information-sharing and transparency.
Plan often	• Identify sustainable funding for existing and future public safety communications priorities. • Oversee and align activities to communications interoperability strategic plans (e.g., Statewide Communication Interoperability Plans and the *National Emergency Communications Plan*).

SOURCE: SAFECOM and National Council of Statewide Interoperability Coordinators, 2018.

Incident-Based Reporting System or a given state-specific version. Given our heavy sampling of California agencies, another regulatory uncertainty was compliance with the state's Racial and Identity Profiling Act (RIPA), which passed in 2015 (State of California, 2015). This law requires police officers to record the perceived race, gender, language abilities, and age of a suspect during every stop along with the reason for a stop, whether a search was conducted, and the results from the search (State of California, 2015). Compliance concerns affect broadband usage because agency decisionmakers are cautious about investing time and money into adopting a new technological system without being certain that their solution would be compliant for the technology's full life cycle. Compliance concerns then factor into decisions around computer-aided dispatch (CAD) systems and records management systems (RMS), which in turn affect an agency's hardware preferences for what is compatible and effective for officer use in the field.

Agencies must operate within the constraints posed by budgets, compliance, and effectiveness in deciding what broadband use cases, if any, are most effective for their needs. The following section demonstrates the variety of ways that broadband services and devices can be used in the different scenarios that agencies face.

Applied Model Use Cases for Broadband

The first step for governing bodies in developing strategic plans is to determine what they want their broadband networks to do to meet their communities' needs. They need to identify the applied use cases describing what their broadband networks will be used for and then analyze those use cases to understand the specific capabilities and enabling hardware, software, and technology services that they need. The following sections discuss common model use cases for broadband networks and high-level network architectures (including devices in the field, communications infrastructure, software, and services) that make them work.

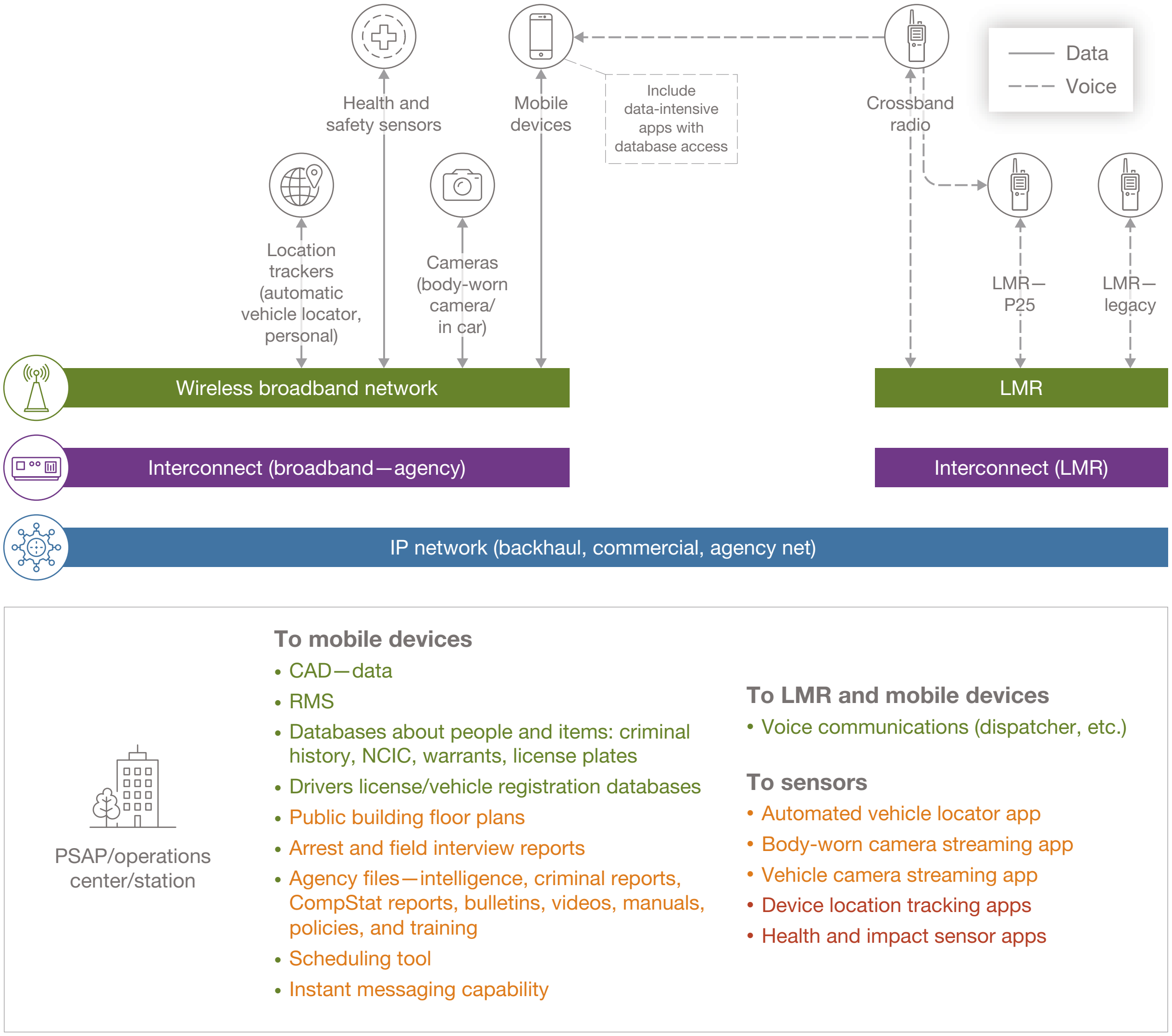
These use cases can be divided into two large categories. The first covers broadband in support of routine policing activities. The second covers broadband in support of major police responses outside the scope of routine policing, including to mass attacks, major events, and natural disasters.

Daily Operations for Patrol Officers

This case, shown in Figure 4.1, reflects the day-to-day operations of officers in the field—supporting officers on patrol, responding to routine calls, conducting stops, and conducting field investigations. Most communications exchanges follow a client-server arrangement, in which officers in the field frequently receive data from and upload data to their agency's PSAP or operations center, or both, via a broadband-to-internet interconnection. Similarly, sensors in the field also upload data back to the PSAP, operations center, or both; sensors directly related to day-to-day operations include location trackers, cameras, and health and safety sensors. In addition to PSAP and operations center exchanges, this use case includes routine unit-to-unit communications, over both broadband and LMR voice channels, with an interconnection between them.

FIGURE 4.1

Broadband Applied Use Case for Routine Policing


Health and safety sensors
Mobile devices
Include data-intensive apps with database access
Crossband radio
Data
Voice
Location trackers (automatic vehicle locator, personal)
Cameras (body-worn camera/ in car)
LMR—P25
LMR—legacy
Wireless broadband network
LMR
Interconnect (broadband—agency)
Interconnect (LMR)
IP network (backhaul, commercial, agency net)
PSAP/operations center/station

To mobile devices

- CAD—data
- RMS
- Databases about people and items: criminal history, NCIC, warrants, license plates
- Drivers license/vehicle registration databases
- Public building floor plans
- Arrest and field interview reports
- Agency files—intelligence, criminal reports, CompStat reports, bulletins, videos, manuals, policies, and training
- Scheduling tool
- Instant messaging capability

To LMR and mobile devices

- Voice communications (dispatcher, etc.)

To sensors

- Automated vehicle locator app
- Body-worn camera streaming app
- Vehicle camera streaming app
- Device location tracking apps
- Health and impact sensor apps

NOTES: NCIC = National Crime Information Center. Green text indicates services that have been identified as central to routine operations. Orange text shows services that have been identified as useful during routine operations but are less central. Red text shows services that are emerging for law enforcement.

The PSAP or operations center hosts a series of communications and data services, with most of the latter applying to officers' mobile devices (e.g., smartphones, tablets, MDTs).[3] Services shown in green are those that have been identified in past research as being central to routine operations; these services, such as CAD, RMS, drivers, and criminal information databases, largely apply to processing enforcement contacts in the field.

Services shown in amber are those that have been identified as being useful during routine operations but are less central. For the mobile user, these tend to be reference materials, such as agency files on past incidents, public building floor plans, and administrative services (e.g., scheduling tools). For the operations center, these are video streams and location sensors from the field.

Finally, the services shown in red are emerging for law enforcement. These are on the officer health and safety side; they include health apps that stream alerts to operations centers, impact sensor apps that stream alerts to operations centers, and individual device location-tracking apps.

Major Criminal Responses

This use case, shown in Figure 4.2, reflects the immediate response to a major criminal incident, such as a shooting or a violent robbery. In this case, agencies need broadband capabilities to help detect the incident as quickly as possible, coordinate the response, secure the scene, and immediately hold offenders accountable by providing clues about perpetrators on scene. Agencies can also use broadband to perform "virtual pursuits," following fleeing vehicles and persons of interest and coordinating responding units. Tracking fleeing vehicles via broadband enables a safer response to this type of incident, which otherwise introduces danger to officers, suspects, and bystanders. This means adding several types of external sensors that can provide situational awareness to officers at all levels as supplemental exchanges:

- shot detection
- surveillance camera photos and feeds
- license plate reader feeds
- UAS and unmanned ground systems (UGS) video feeds.

This use case sees an increased number of information and document requests between officers in the field and analysts and staff at headquarters, dispatch, and operations centers. Conversely, some tools and repositories for routine policing, such as administrative and data access tools, do not apply in this use case (or at least not as much) and are excluded from the figure.

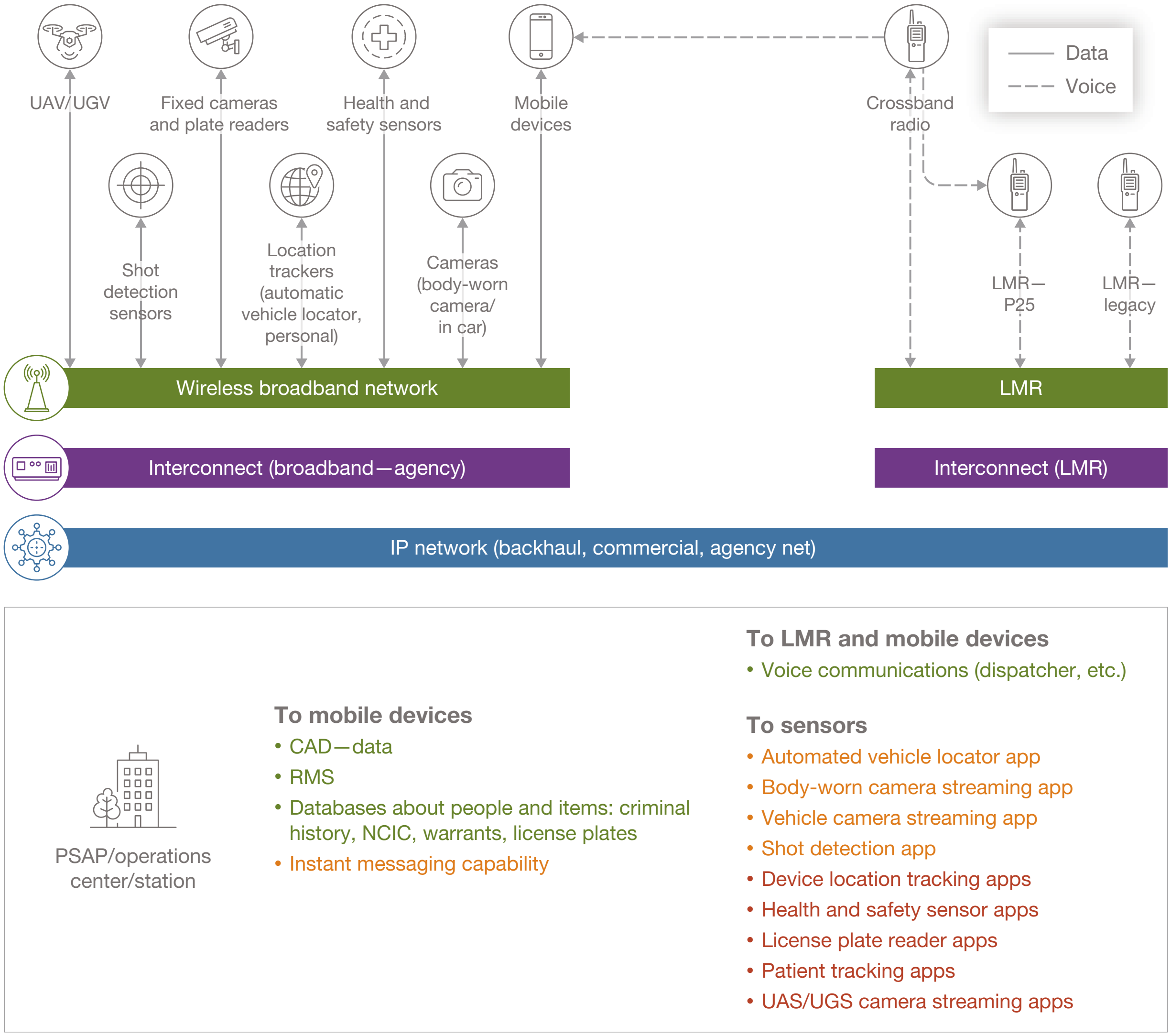
Mass Attack Responses

This use case, shown in Figure 4.3, is part of the second large category discussed earlier, which focuses on major incident and event responses outside of routine policing. The first of these, the mass attack response use case, builds on major criminal response. In this case, the massive scale of the response means that incident command and situational awareness of the units involved are paramount concerns.

Core to this use case is maintaining awareness and communications in two ways. The first is preemption for first responders, which is critical because many bystanders will be present who will try to communicate

[3] The PSAP and operations center information services and their characterizations summarize past analyses on information exchange needs, notably the past National Institute of Justice (NIJ)–funded expert panel on needs for law enforcement broadband (Hollywood et al., 2016) and a prior NIJ-funded technology assessment of law enforcement information exchange issues and needs (Hollywood and Winkelman, 2015).

FIGURE 4.2
Broadband Use Case for Major Criminal Responses


Data
Voice
UAV/UGV
Fixed cameras and plate readers
Health and safety sensors
Mobile devices
Crossband radio
Shot detection sensors
Location trackers (automatic vehicle locator, personal)
Cameras (body-worn camera/ in car)
LMR—P25
LMR—legacy
Wireless broadband network
LMR
Interconnect (broadband—agency)
Interconnect (LMR)
IP network (backhaul, commercial, agency net)
PSAP/operations center/station

To mobile devices

- CAD—data
- RMS
- Databases about people and items: criminal history, NCIC, warrants, license plates
- Instant messaging capability

To LMR and mobile devices

- Voice communications (dispatcher, etc.)

To sensors

- Automated vehicle locator app
- Body-worn camera streaming app
- Vehicle camera streaming app
- Shot detection app
- Device location tracking apps
- Health and safety sensor apps
- License plate reader apps
- Patient tracking apps
- UAS/UGS camera streaming apps

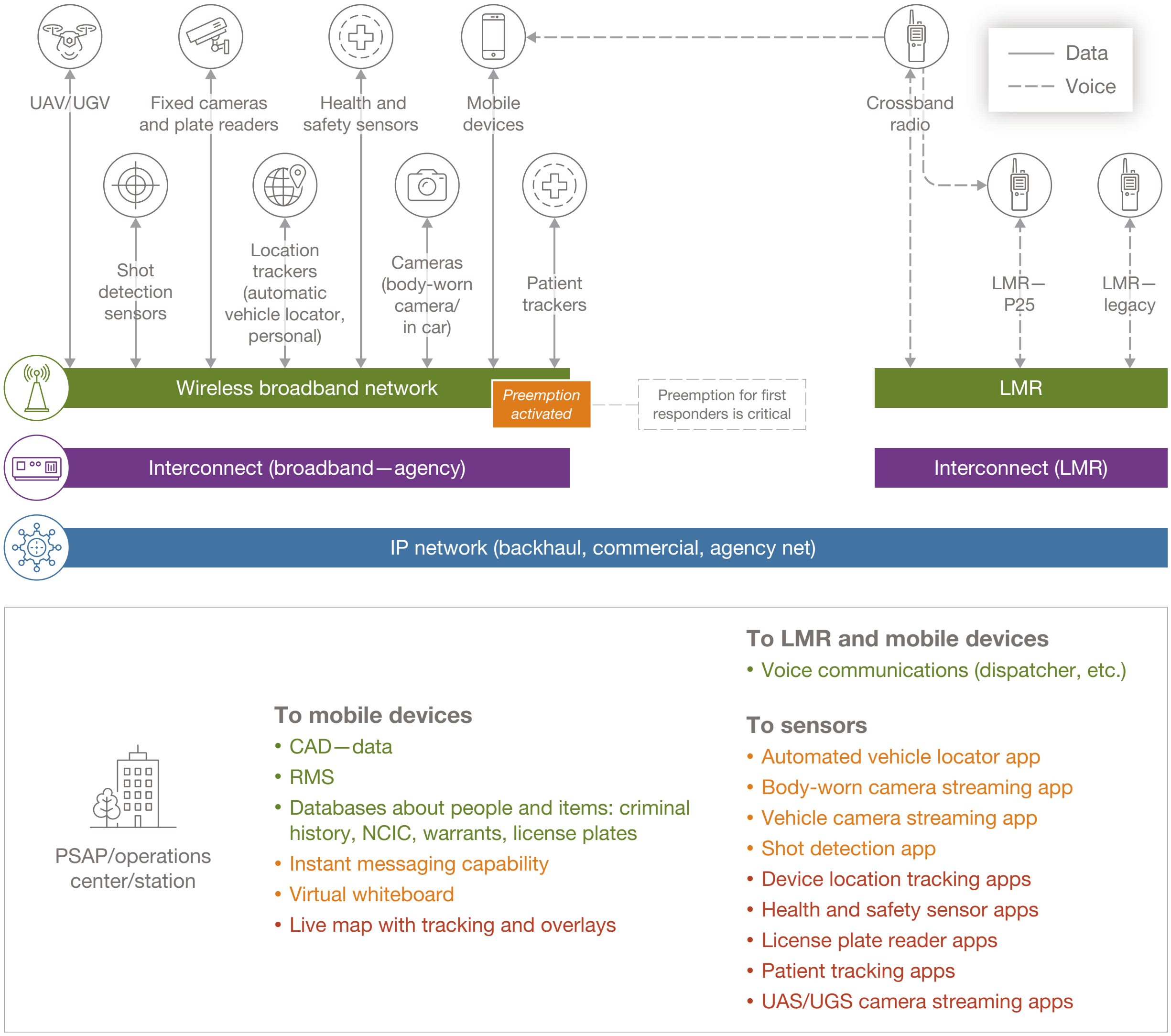
NOTE: Green text indicates services that have been identified as central to routine operations. Orange text shows services that have been identified as useful during routine operations but are less central. Red text shows services that are emerging for law enforcement.

at once, possibly overloading commercial networks with calls, posts, and streaming video. The second is that there is a pressing need for first responders to avoid swamping the voice communications network by trying to communicate at once on shared PTT channels. This is, in part, a radio discipline issue, but there are software tools that share awareness and direction that reduce the need for voice communications. The Route 91 Harvest Festival mass shooting in 2017 provides clear examples of this situation. Some key observations are that (1) fire department mobile computer terminals had issues with uploading information, (2) first responders were unable to transmit or receive information, and (3) radio traffic was congested.

For mass attack and similar emergency events, major capabilities are needed, and the specific broadband sensors and communications devices supporting them include the following:

FIGURE 4.3

Broadband Use Case for Mass Attack Responses


UAV/UGV
Fixed cameras and plate readers
Health and safety sensors
Mobile devices
Crossband radio
Data
Voice
Shot detection sensors
Location trackers (automatic vehicle locator, personal)
Cameras (body-worn camera/ in car)
Patient trackers
LMR—P25
LMR—legacy
Wireless broadband network
Preemption activated
Preemption for first responders is critical
LMR
Interconnect (broadband—agency)
Interconnect (LMR)
IP network (backhaul, commercial, agency net)
PSAP/operations center/station
To mobile devices
• CAD—data
• RMS
• Databases about people and items: criminal history, NCIC, warrants, license plates
• Instant messaging capability
• Virtual whiteboard
• Live map with tracking and overlays
To LMR and mobile devices
• Voice communications (dispatcher, etc.)
To sensors
• Automated vehicle locator app
• Body-worn camera streaming app
• Vehicle camera streaming app
• Shot detection app
• Device location tracking apps
• Health and safety sensor apps
• License plate reader apps
• Patient tracking apps
• UAS/UGS camera streaming apps

NOTE: Green text indicates services that have been identified as central to routine operations. Orange text shows services that have been identified as useful during routine operations but are less central. Red text shows services that are emerging for law enforcement.

- to gain direct awareness of where shooters and victims are
  - cameras, including access to surveillance cameras already in the location (which typically means getting access to those cameras' IP streams) and the agencies' own fixed and mobile cameras
  - shot spotting alerts
- to know where units are, as well as their status
  - location trackers on vehicles and officers
  - location-tracking features on officers' mobile devices
  - health and safety sensors
  - situational awareness display software, for commanders both at operations centers and in the field to see where all units are on a map display
  - for incidents in major public buildings: databases of public building floor plans, integrated with the map displays (so that unit locations and operational areas can be overlaid on floor plans)

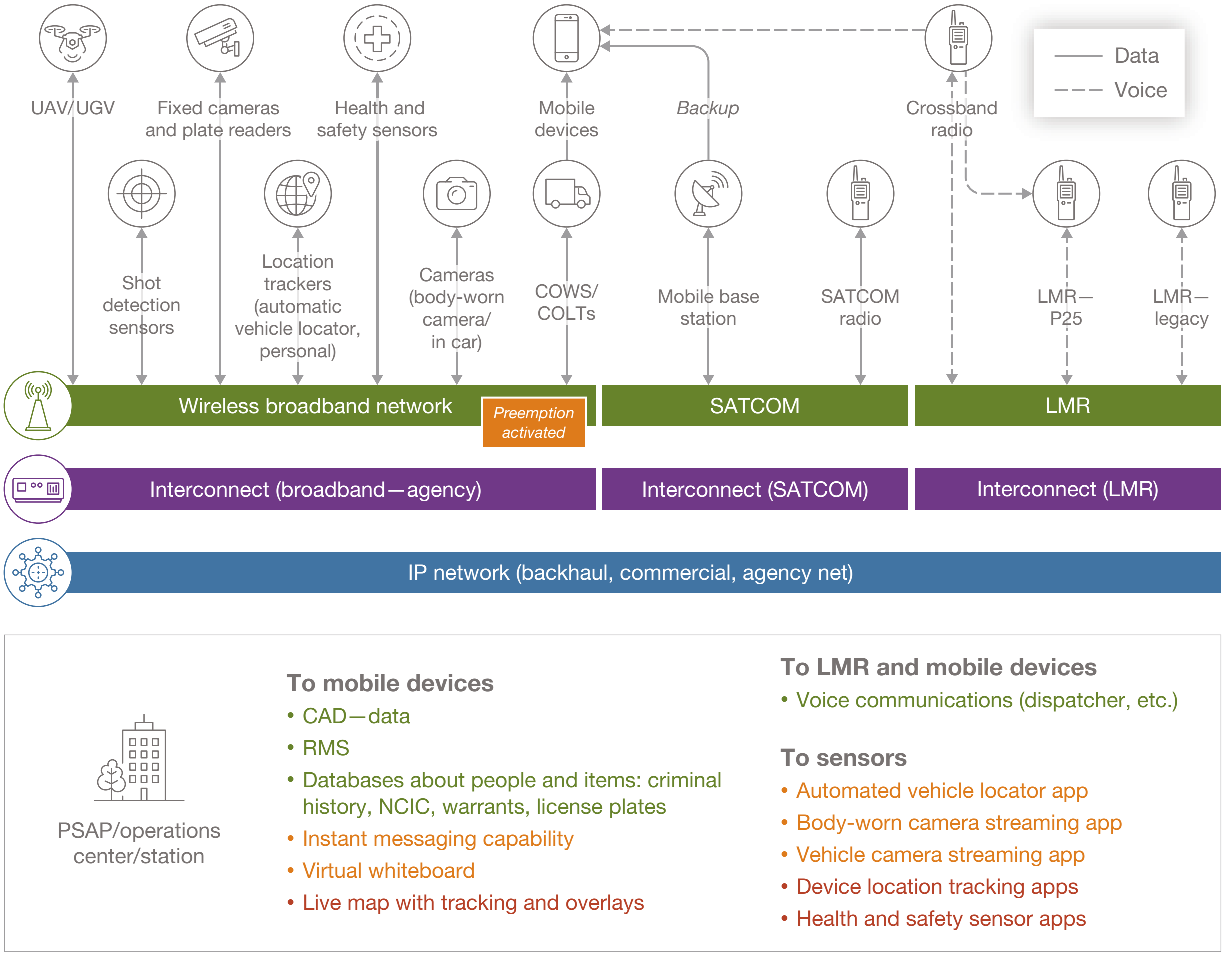
- to share situational awareness, updates, and orders to avoid overwhelming radio communications
  - direct and group instant messaging
  - shared virtual whiteboards, in which officers can collectively see posted updates
  - maps with overlays showing key locations, operational areas, and unit locations
- to determine the whereabouts of victims
  - patient tracking systems (an emerging technology)[4]
- to provide voice communications
  - broadband devices with PTT and legacy LMR, integrated into common voice channels.

Major Event Security

The major event security use case, shown in Figure 4.4, is somewhat similar in character to the mass public attack use case in terms of the scale and the number of units and resources involved, as well as the informa-

FIGURE 4.4

Broadband Use Case for Major Event Security


UAV/UGV
Fixed cameras and plate readers
Health and safety sensors
Mobile devices
Backup
Crossband radio
Data
Voice
Shot detection sensors
Location trackers (automatic vehicle locator, personal)
Cameras (body-worn camera/ in car)
COWS/ COLTs
Mobile base station
SATCOM radio
LMR—P25
LMR—legacy
Wireless broadband network
Preemption activated
SATCOM
LMR
Interconnect (broadband—agency)
Interconnect (SATCOM)
Interconnect (LMR)
IP network (backhaul, commercial, agency net)
PSAP/operations center/station

To mobile devices
- CAD—data
- RMS
- Databases about people and items: criminal history, NCIC, warrants, license plates
- Instant messaging capability
- Virtual whiteboard
- Live map with tracking and overlays

To LMR and mobile devices
- Voice communications (dispatcher, etc.)

To sensors
- Automated vehicle locator app
- Body-worn camera streaming app
- Vehicle camera streaming app
- Device location tracking apps
- Health and safety sensor apps

NOTE: Green text indicates services that have been identified as central to routine operations. Orange text shows services that have been identified as useful during routine operations but are less central. Red text shows services that are emerging for law enforcement.

[4] Victim identification and tracking can augment or supplant paper tracking systems, allowing for close monitoring of an incident on scene, assisting hospitals, and helping family members or investigators locate victims after transport.

tion technology (IT) capabilities needed. As in the mass attack use case, preemption will be needed to prevent first responder communications from being overwhelmed by spectators' calls, posts, messages, and live streams. There are also similar issues with having inadequate communications capacity, in this case more from the sheer number of partner units involved. This use case, however, does have the advantage of advance planning for the event, so the architecture involves bringing in portable communications towers and infrastructure (e.g., COLTs, COWs, aerial relays, SATCOM) as needed. For example, for major events, such as the Super Bowl, COWs and SatCOLTs are deployed to assist first responders (Adams, 2021).

There are also similar needs for providing awareness of units' locations and statuses, the security picture at the event, and sharing orders. However, in contrast to the mass attack use case, this use case does not have a need for victim tracking (unless a major incident occurs at the event).

Disaster Responses Requiring Portable Communications Infrastructure

This use case, shown in Figure 4.5, is similar in character to the previous two in that it involves a very large public safety response and has substantial needs for sharing situational awareness information, including unit locations and statuses, victim tracking information, and the overall security picture of the disaster response.

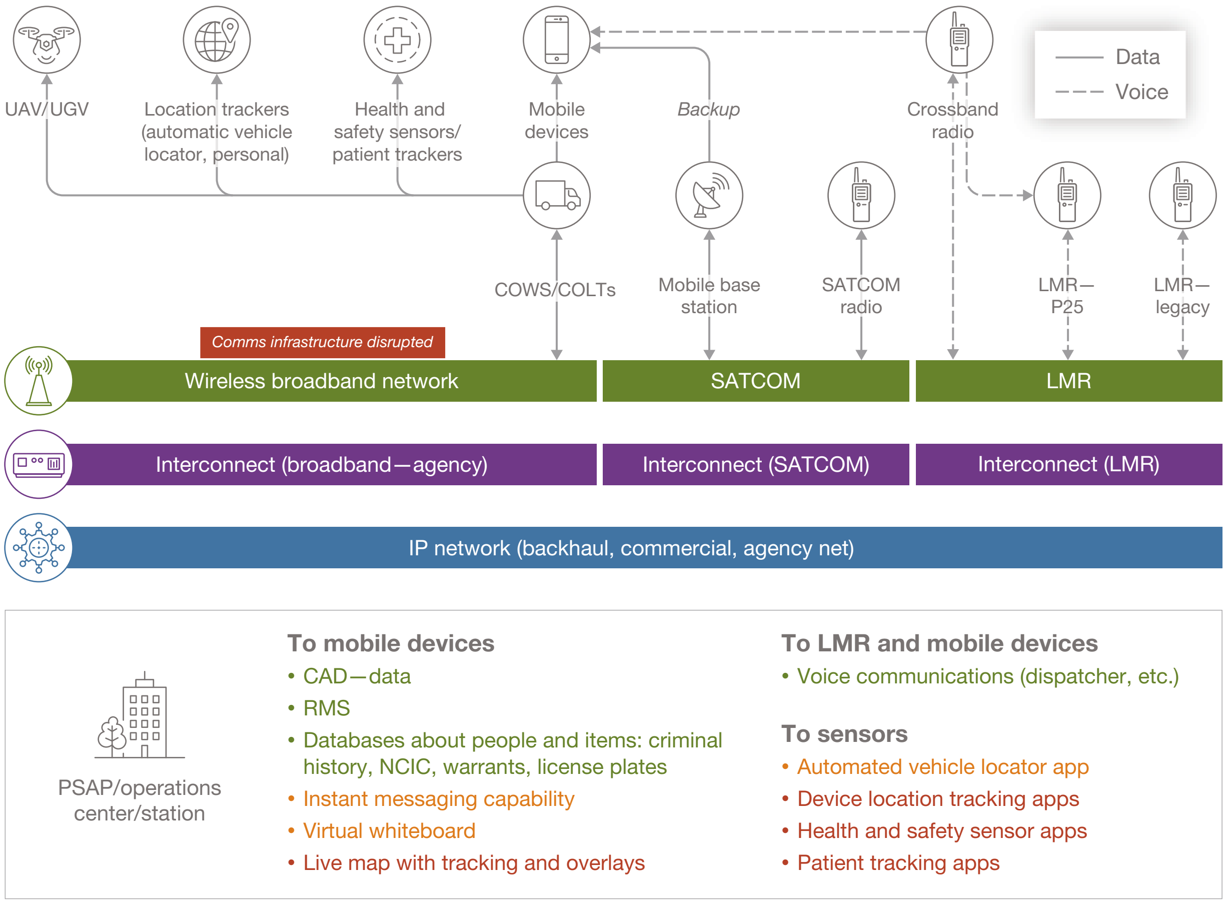
The major complication in this use case is that most of the existing communications infrastructure is nonfunctional because of the disaster. Whereas, in the major event case, the portable communications systems are supplemental, in this case they form the bulk of the communications network. This case requires being able to provide sufficient portable communications infrastructure, whether from COLTs, COWs, relays, or SATCOM vehicles and stations, to support a large-scale disaster response.

The key services supported in this scenario are those anticipated for a natural disaster response that disrupts LMR/broadband cell towers or communications systems. These services focus on coordinating the overall response (virtual whiteboard, instant messaging), tracking units (maps with unit tracking and overlays), and managing interactions with health and safety apps used for patient care and tracking.

In addition to a "traditional" disaster response, such as to wildfires, floods, or hurricanes, planners and first responders must understand the limitations of a portable communications infrastructure if those systems are used to notify the public of actual or imminent danger. For instance, in 2018, the Camp Fire in Butte County, California, destroyed the town of Paradise and killed 85 people. The sheriff's department had the capability to send zone-by-zone mass messages to Paradise residents via telephone to warn them of the approaching fire; however, fewer than half of the 26,000 residents had signed up for the service. As conditions worsened, the sheriff's office attempted to use the Federal Emergency Management Agency's (FEMA's) Integrated Public Alert and Warning System to send wireless texts, but those attempts were not successful. In total, only 7,000 of the 52,000 residents who evacuated the affected area received alerts about the danger. This tragedy highlights the unpredictable ways in which communications systems can fail in practice. The software that the county used did not work as intended, communications cables and cell towers were rapidly damaged, and the coordination among county and federal agencies did not generate the hoped-for FEMA wireless emergency (text) alerts (WEA).[5] The Camp Fire and similar events are useful in considering the gaps between intent and reality and serve as case studies as agencies "pressure test" their own emergency communications.

[5] There are many reports and articles about the Camp Fire. The source that we used is PBS's *Frontline*, which investigated the disaster as part of the preparation for the documentary *Fire in Paradise* (Todd, Trattner, and McMullen, 2019), which aired in 2019.

FIGURE 4.5
Disaster Responses Requiring Portable Communications Infrastructure


Data
Voice
UAV/UGV
Location trackers (automatic vehicle locator, personal)
Health and safety sensors/ patient trackers
Mobile devices
Backup
Crossband radio
COWS/COLTs
Mobile base station
SATCOM radio
LMR—P25
LMR—legacy
Comms infrastructure disrupted
Wireless broadband network
SATCOM
LMR
Interconnect (broadband—agency)
Interconnect (SATCOM)
Interconnect (LMR)
IP network (backhaul, commercial, agency net)
PSAP/operations center/station
To mobile devices
• CAD—data
• RMS
• Databases about people and items: criminal history, NCIC, warrants, license plates
• Instant messaging capability
• Virtual whiteboard
• Live map with tracking and overlays
To LMR and mobile devices
• Voice communications (dispatcher, etc.)
To sensors
• Automated vehicle locator app
• Device location tracking apps
• Health and safety sensor apps
• Patient tracking apps

NOTE: Green text indicates services that have been identified as central to routine operations. Orange text shows services that have been identified as useful during routine operations but are less central. Red text shows services that are emerging for law enforcement.

Broadband Considerations in Fire and Emergency Medical Services

Although many of the considerations described in this report apply to all emergency response entities, fire and emergency medical response organizations face their own needs and challenges. For many users, these operational considerations amount to the largest single factor affecting any decisions around broadband communications. One interviewee from a Southern California fire department likened an end user's use of communications technology to turning on a kitchen faucet—as long as water comes out safely and reliably, the system of pipes and waterworks that got it there is not notable or important.

That said, certain operational considerations do come into play when all-hazard fire and EMS departments adopt broadband communications technology, be it from FirstNet or from a competing provider. Long reliant on interlocking LMR systems capable of communicating with neighboring jurisdictions in an agreed-upon set of communications and frequency plans, fire authorities whom we interviewed expressed a preference for the redundancy and reliability of existing voice communications technology supplemented, rather than replaced by, cellular or broadband-based devices.

More promising than advanced PTT capability for fire departments are likely the capabilities that broadband devices offer in resource tracking and safety. Such technology as tablet computer–based incident management systems offering greater command and control and *z*-axis (in-building tracking technology) and the firefighter safety that it might offer were both specifically mentioned in interviews.

In choosing a level of cellular broadband service and choosing a provider, coverage availability is normally the primary concern driving decisions. As network parity was reached in certain metro areas—including around one interviewed department in the southwestern United States—other concerns, such as cost and redundancy, began to dominate decisionmaking. Rather than voicing specific concerns about Band 14 availability, fire department users described the end-user goals of reliability and preemption availability as their primary points of interest. Navigating this decision process was a concern among interviewed local fire department officials, who specifically mentioned aggressive sales pitches and inattentive customer support. An interviewee from one department pointed to the department's large size and personal relationship with provider personnel as the primary reasons that they could navigate the process successfully at all.

CHAPTER FIVE

Funding and Acquisition

Once an agency knows how it wants to use communications technology, it needs to determine how to pay for and acquire the needed capabilities. In this chapter, we introduce important considerations for agencies and funding authorities, such as cities and counties. We have based these considerations on responses from our interview sample, which consists of police leadership, administration, and civilian staff in agencies in one northeastern state and one western state. We first discuss sources and mechanisms for funding communications technology, and we then describe agencies' experiences with the acquisition process.

Funding Sources

Our interviews identified several ways in which to fund and acquire communications technologies, such as LMR, dispatch consoles, and MDTs. Respondents indicated that the funding tended to fall into police or city budget authority, which in some cases has been predicated by the amount requested. Specifically, we examined whether the participants noted the use of a dedicated IT budget; an annual budget; an operating budget; state purchasing contracts; or other funding mechanisms, such as grants or donations. Not all interviewees went into great detail about funding sources, but, where information was available, we have included it in this section. Table 5.1 summarizes the funding sources identified in the interviews.

As shown in Table 5.1, there are four main budget types that were discussed in interviews with law enforcement. First, seven interviewees discussed having a dedicated IT budget. In these cases, some of the IT budgets are located at the city or municipality level, which helps fund some portions of police communications tech-

TABLE 5.1

Types of Funding Sources Identified in Interviews

Code	Meaning	Number of Interviewees Who Responded Affirmatively
Dedicated IT budget	Does the agency have a dedicated IT budget?	7
Annual budget	Does the agency use a normal annual municipal budgeting process, typically for larger-capital planned purchases?	12
Operating budget	Does the agency use its operating budget, typically for a smaller unplanned purchase or purchases?	8
Grants	Does the agency use grants to fund IT/communications needs?	7
Private donations	Does the agency use private donations to fund IT/communications needs?	1

NOTE: Respondents could indicate more than one funding mechanism.

nology, such as computers and network support.[1] Continuing this trend, in the case of one West Coast city, a central IT department makes the purchases, *but* there are personnel in each department that understand their agency's specific needs.[2] This structure can be helpful to assist in conveying and relaying public safety needs to the city as a whole. In another agency, larger purchases must go through the city, including systems related to phone, email, and the physical network.[3]

Respondents also indicated that funding comes from an annual budget or operating budget. As with the dedicated IT budget responses, these groupings are not mutually exclusive. For annual budgets, the study team assessed when an agency indicates that it can (or has) used its department's annual budget process to fund and purchase communications technologies. For operating budgets, we examined whether smaller purchases could be completed using an agency's day-to-day budget.

Generally, the responses fit into this schema of separating larger from smaller purchases. In one case, a respondent noted that they "don't have a dedicated IT budget; [these expenditures] come out of the general ops budget, which is about $15 million."[4] One agency noted a combined approach to fund its needs: "ops budget, chief allocates money each year, [we] also have a grant for an IT project. Sometimes at the end of the fiscal year there may be money left over, and it becomes a little mini competition—what are the priorities, what do we need to get done?"[5] In comparing budget needs, a participant noted that the cost of radios is a massive capital expense compared with the cost of other technology, such as computers.[6] This might push some agencies to include large outlays of funds for annual budgets and to combine those efforts with other sources, such as grants, detailed later in this section.

Seven of our interviews reflected how police agencies have relied on grants to fund communications technology endeavors. Table 5.2 provides examples of relevant comments. The reliance on grants reflects a gap in police (or city and county) budgets that must be filled to equip officers or update communications technology. Accordingly, it could be difficult for agencies to fund projects without seeking external monies.

Interestingly, significant amounts of attention and resources have been dedicated to assisting law enforcement agencies in securing grant funding specific to communications technology. Several articles discuss FEMA and, more broadly, other U.S. Department of Homeland Security grants to help with needs (Gallagher, 2018; FEMA Grant Programs Directorate, 2021; FEMA Grant Programs Directorate, 2022). This is consistent with what we heard from the chief of police for a police department in Southern California in an interview in January 2020. However, Stockton (2019) notes that the period in which to apply for grants can be relatively short. Therefore, in terms of funding FirstNet or other technologies, police departments must be prepared to apply for grant assistance when it becomes available. FEMA's *Preparedness Grants Manual* (FEMA Grant Programs Directorate, 2021) outlines how and where grants can be used by agencies to support FirstNet technologies, such as integration of IT infrastructure, handheld or vehicle-based devices, and accessories to support devices (e.g., headsets, cases).

Other federal grant programs, including the Edward Byrne Memorial Justice Assistance Grant (JAG) Program, make specific reference to FirstNet and interoperable communications technology. For example, the FY 2019 Byrne Grant states, "For JAG applicants considering implementing communications technology

[1] Interview with the head of technology for a police department in Massachusetts, February 7, 2020.

[2] Interview with the business services administrator for a police department in Southern California, January 29, 2020.

[3] Interview with the IT manager and chief of innovation for a police department in Southern California, January 31, 2020.

[4] Interview with administrative captain for a police department in Southern California, January 28, 2020.

[5] Interview with system administrator for a police department in Massachusetts, January 29, 2020.

[6] Interview with system administrator for a police department in Massachusetts, January 29, 2020.

TABLE 5.2
Sample Comments Regarding Grants to Support Communications Technology

Interviewee, Organization, State, and Interview Month and Year	Comment
Management at a joint-powers agreement in CA, April 2019	"Grant money to help PDs transition is also critical, as many departments don't have the funds."
System administrator, PD in Southern CA, January 2020	"[We] also have a grant for an IT project. Sometimes at the end of the fiscal year there may be money left over, and it becomes a little mini competition—what are the priorities, what do we need to get done?"
Chief of police, PD in MA, February 2020	"We also utilize state grants."
IT manager, PD in Southern CA, January 2020	"We use the general budget—[it] generally has to be planned; and we can leverage funds from Measure A [people] and Measure P [infrastructure]—these are tax initiatives. Sometimes it's from asset seizure, and then also grants."
Head of technology, PD in MA, February 2020	"Extra technology—different grants, budget into the police budget. The source of funds really depends on what money is available."
Chief of police, PD in MA, February 2020	"Have used grants in the past—purchased about four or five tablets and associated applications with that. Certain grants [are] only eligible every so many years—we got maybe $22,000."
Chief of police, PD in Southern CA, January 2020	Question: "Where do you get grants from?" Answer: "Homeland Security for some."

NOTES: CA = California; MA = Massachusetts; PD = police department. City and agency names are withheld to protect interviewees' anonymity.

projects, it is worthwhile to consider the First Responder Network Authority (FirstNet) Program" (Bureau of Justice Assistance, 2019, p. 9).

Lastly, one of the agencies included for analysis indicated that it was able to use private-citizen donations over and above its other funding sources. Although this might not be feasible in many areas, it does represent a potential way to fulfill agency and communications needs.

Table 5.3 shows the department communications budgets described in the interviews. To provide a point of comparison, we have also included a range of exemplar department operating budgets in the table for police departments, since it can guide the different abilities to fund communications technology.

Whereas a larger agency has a higher per-employee budget (based on 2016 Law Enforcement Management and Administrative Statistics data; see Bureau of Justice Statistics, undated), smaller agencies can make the use of funds for FirstNet or other communications technology untenable. The additional strains on law enforcement budgets, whether caused by tax shortfalls or defund or reallocation efforts, could further affect the ability to purchase, maintain, and upgrade communications technology.

Funding authorities need to be aware that budgeting for broadband communications requires a broader scope than the typical wireless contract. In budgeting for broadband networks, funding authorities need to include the following:

- **software on the devices (apps)**, including existing software apps or, depending on the agency's needs, new software (or at least customizations of existing software that require new coding), which requires budgeting for developing and testing.
- **connections between the mobile apps and back-end databases**, especially CAD/RMS and the mobile app for displaying and querying CAD/RMS data. (Depending on the vendor, the CAD/RMS mobile connections might be included as part of app deployment agreements, might require extra costs, or might require custom builds).

TABLE 5.3
Department Communication Budgets Described in Interviews

Population Served	Department Budget (Total)	Per-Employee Budget
1,000,000 or more	$977,064,539	$142,617
500,000–999,999	$253,761,582	$130,540
250,000–499,999	$109,685,085	$130,411
100,000–249,999	$43,714,559	$134,860
50,000–99,999	$20,112,984	$132,000
25,000–49,999	$8,790,977	$116,431
10,000–24,999	$4,185,582	$104,846
2,500–9,999	$1,319,686	$81,009
2,499 or fewer	$300,802	$54,130

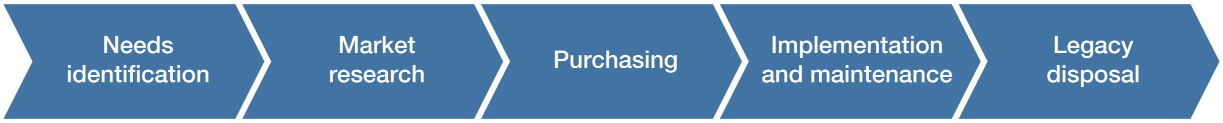
SOURCE: Brooks, 2020.

- **mobile device management (MDM) systems**, which provide administration and configuration control over the mobile devices on an agency's broadband network.
- **mobile application management (MAM) systems**, which automatically update and manage the apps on the mobile devices on an agency's broadband network.
- **bridging to LMR networks**, used in acquiring and maintaining whatever bridging technology is being used (IP solutions and/or donor radios or hardware gateways).
- **training**, including developing and/or acquiring training materials for the apps in use, updated voice communications procedures, and cybersecurity policies and procedures.
- **personnel to oversee the fielding and maintenance** of wireless equipment.
- **personnel to oversee the software and network administration** of the apps and data going across the broadband network. This work must include cybersecurity provisions, including both cyber defense and strong resilience and backup capabilities.

Acquisition

We provided interviewees with a theoretical framework for the acquisition of various communications technologies (see Figure 5.1). We then used this framework in our interviews with police agencies to understand the stages in this process and to identify trends and best practices in acquisition.

FIGURE 5.1
Theoretical Acquisition Framework



Needs Identification

During interviews, we asked agency representatives how they identified various needs. Although we could not identify a pattern or clear process from our interviews, there are some important techniques that we uncovered. For example, several agencies noted that patrol officers or officers in the field identified or voiced their needs, which helped drive decisionmaking and additional research. Interviewees, whether law enforcement executives or IT staff members, noted that they had some ability to make suggestions or decisions at this stage of the acquisition process. However, no pattern emerged as the predominant process for identifying needs. Table 5.4 includes sample interview comments that support this notion.

TABLE 5.4

Sample Comments on Needs Identification

Interviewee, Organization, State, and Interview Month and Year	Comment
Head of technology, PD in MA, February 2020	“[Needs/ideas] typically come from superior officers [e.g., the chief learns from conferences], but also I will suggest stuff like software upgrades; officers in the field [also identify needs].”
IT liaison, PD in CA, January 2020	“We look forward to some degree. [For] example, electronic ticket writers—I proposed this idea to [the] PD, and we are moving forward with it. In order for things to move forward, I need our sponsor to back up the idea. The whole organization is on a tight budget, so they need control over where the dollars are being spent. Patrol officers are pushing it, and we try to do the best we can to accommodate all the requests.”
Chief of police, PD in Southern CA, January 2020	“There [is] no single way of identifying; sometimes it’s just an officer in the field saying, ‘I need this.’ Being small lets us pull the trigger faster. We say, as a command staff, ‘That seems like a good idea’; we can just go out and get it. Replacing all in-car trunked systems. If something goes out to bid, the city council will be involved; [we] have to ask for approval to put out an RFP.”
Administrative captain, PD in Southern CA, January 2020	Q: “Who is responsible for needs identification?” A: “Everything falls on me as the admin captain.”
Business services administrator, PD in Southern CA, January 2020	“No clear or linear process. It’s an ongoing process where there are constantly needs being identified, piloted, and purchased throughout the department. We operate with a central IT department, but there are liaisons between IT and each business unit to coordinate decisionmaking.”
Administrative personnel, PD in Southern CA in January 2020	“[Needs identification is] user driven more than anything.”
IT manager, PD in Southern CA, January 2020	“Ideas come from sergeants, retired captains, come from me, from across the department. This has changed since I was hired five years ago; as the department has seen our ability to execute on technology, more and more people [are] coming forward asking for things.”
Chief of police, PD in MA, February 2020	“We get feedback from officers in the field. . . . dispatch fire department and EMS so we try to get input from them for their needs.”
Administrative LT, PD in MA, February 2020	“[We] wait until something falls apart and doesn’t work; we are trying to be forward thinking, send people to conferences, meet with vendors. We have all of our basic needs met, but as technology changes we try to look at whether there’s something out there that can improve operations. Get people together to talk about whether something is really going to get used.”
Chief of police, PD in MA, February 2020	“On a yearly basis, we look at aging on equipment—wear and tear and needed upgrades—and see what needs to be phased out. Police budget line takes care of this.”

NOTES: CA = California; LT = lieutenant; MA = Massachusetts; PD = police department. City and agency names are withheld to protect interviewees’ anonymity.

Market Research

After the discussions on needs identification, we sought to understand how agencies then took steps to conduct market research. Our interviews yielded seven results that were substantially related to market research that could be helpful in guiding the acquisition process.

Some of the interviewees said that their agencies rely on going to conferences to see what types of technology are available, but they also indicated that they vet technology, either in house or by contacting other nearby agencies. Sample comments are shown in Table 5.5.

TABLE 5.5

Sample Comments on Market Research

Interviewee, Organization, State, and Interview Month and Year	Comment
Head of technology, PD in MA, February 2020	"[We] talk to the surrounding communities; this is my go-to. [A local city police agency] is one department; I frequently reach out to them. Dispatch stuff, I'll talk to officers, meet with vendors, [go to] conferences. Verizon has an innovation center, and they do a public safety fair every year, and there will be lots of vendors there."
Administrative LT, PD in MA, February 2020	"[We] meet with vendors, send people to conferences. Mostly learn about google alerts, newsletters, follow what's going on in the private sector. We try things out before we purchase."
System administrator, PD in MA, January 2020	"[We are] not looking for everything; having all the latest technology is not necessarily our priority—[we] don't need to meet with every salesperson. Often, salespeople say one thing, but we find out that's not really what the technology offers. There's also the practicality of whether it will be used. People just want to be a cop; if what you are trying to use [or] implement is a hindrance to doing their job, they won't want to do it." A vendor will say, 'It's simple to use,' but, for us, it's not. There are some things that you need to be able to do, [like] create a map; [we] need to have applications to do that, but for certain things you don't need everyone to know."
Admin personnel, PD in Southern CA, January 2020	Q: "What other technology have you looked into?" A: "We have looked into cloud storage, but there's currently no CAL-DOJ–compliant service because you have to know the location of your data. Perhaps this will change in the future, but, until then, no. CAL-DOJ compliance affects other decisions as well. We struck an agreement with Verizon to be a micro cell test market, free easements in exchange for backhaul."
IT manager, PD in Southern CA, January 2020	"I do a little research into what's out there; I ask questions to understand better what we are trying to achieve. If it doesn't exist, can we build it? I do a lot of vetting of technologies."
Chief of police, PD in MA, February 2020	"[We conduct] background research, ask around if other local agencies have it or have looked into it."
Chief of police, PD in MA, February 2020	"I attend trade shows and conferences yearly, [such as the] FBI national academy and IACP [International Association of Chiefs of Police] conferences. [We] stuck with FirstNet for [the following] reasons: Band 14, Motorola on portables, and MDTs: [We] went from Panasonic Toughbooks to mobile PC, more of a tablet."
IT personnel, sheriff's department in Southern CA, April 2020	"We learn from each other; that's where we have the most credibility. We are doing tours; we spend plenty of time going and looking out at other places, too. It's challenging because there's always a vendor out there that wants to sell you something. But we don't want to be the first adopter; maybe it works for a small city, two square miles, but, for a large geographic area, large sworn [police officer force], [it's] not a good idea. We should be cautious, watching what other people do but making sure our people have the tools to get the job done. We also do extensive proof-of-concept tests."

NOTES: CA = California; LT = lieutenant; MA = Massachusetts; PD = police department. City and agency names are withheld to protect interviewees' anonymity.

The Role of Consultants

During our interviews, several agencies reported using consultants to guide them through processes and decisionmaking for the acquisition of communications technology. The use of a consultant is not limited to market research but can assist with guiding an agency through the entire process.

Not surprisingly, interviewees said the consultant's role is to be able to assist police with expertise that is outside the law enforcement mission set. In this sense, as an agency is considering massive expenditures for communications technology, using a consultant that specializes in this process could be a beneficial investment. Sample comments are shown in Table 5.6.

We have continued to see the use of consultants in practice to acquire and contract for communications technologies and services. For example, in 2021, the following departments had open RFPs for communications technology or IT consultants:

- **East Windsor, Connecticut:** "The Town of East Windsor is seeking proposals for Professional Consulting Services for an analysis of our current radio system and to prepare recommendations based on the results of the analysis. The successful consultant will enter into a contract that incorporates both the RFP along with the submitted proposal and have the best interest of the Town as a primary goal" (New England Radio Consultants, LLC, 2021).
- **Albany, New York:** "The City of Albany (hereinafter referred to as the 'City') hereby requests Proposals from qualified firms or individuals with experience in Police Department Information Technology ('IT') needs and operations to develop a formal Three-Year Information Technology Strategic Plan for the City of Albany Police Department ('APD') that will assess current functionality and capacity and provide recommendations for future technology needs, based on industry-recommended practices. This shall include, but shall not be limited to, technology systems, telecommunications, hardware, software, and human capital" (City of Albany, New York, 2022).
- **Mequon, Wisconsin:** "This project is seeking the assistance of a consultant to develop an Information Technology Strategic Plan to guide the organization through the next five years, and also to create a more detailed IT infrastructure plan and design. The City reserves the right to reject any or all proposals, to waive any technicality or to accept any proposal considered to be in best interests of City" (City of Mequon, Wisconsin, 2021).

TABLE 5.6
Sample Comments on the Role of Consultants

Interviewee, Organization, State, and Interview Month and Year	Comment
Chief of police, PD in Southern CA, January 2020	"We need someone that understands law enforcement culture and understands what that equipment and technology is going to do in the field."
Business manager, PD in Southern CA, January 2020	"We hired a consultant to guide us through the process for CAD/RMS."
System administrator, PD in Southern CA, January 2020	"We do see a trend in outsourcing IT support; few have networking or application specialists . . . hire these people to run their help desk."
Business services administrator, PD in Southern CA, January 2020	"We used RFPs for the larger acquisitions; those also tend to involve a consultant. Sometimes a separate RFP is used for the consultant."
IT manager, PD in Southern CA, January 2020	"Seems like there should be a way for every agency to chip in money to hire people like me and then, at no [additional] cost, provide recommendations on IT and technology that wouldn't be vendor driven."

NOTES: CA = California; PD = police department. City and agency names are withheld to protect interviewees' anonymity.

The use of a consultant in these cases can complement in-house or outsourced IT or communications technology personnel.

Purchasing

After agencies have identified needs and conducted market research, their next step is to navigate the actual purchasing of the equipment. This part of the process tends to involve some bureaucracy, whether at the local or the state level. For example, some agencies reported needing additional city approval, especially when the level of funding requested was substantial.[7] In other cases, when purchases exceeded a certain threshold, the state procurement system and its rules had to be followed.[8]

Interviewees shared both strengths and weaknesses of having to work through external purchasing systems. In some cases, the purchasing process used was advantageous because of an agency's size,[9] or for convenience,[10] but it could hinder getting the best price.[11] Sample comments are shown in Table 5.7.

Implementation and Maintenance

Additional costs and considerations that should be factored into decisionmaking are how technologies are implemented in departments and what maintenance consists of. While our interviews did not yield a great deal of information about implementing systems or technology, one participant noted that training is an important factor to consider.[12] We also learned that maintenance tends to be outsourced or contracted out of the police department to a vendor.[13] This information suggests that it would be prudent for agencies looking at implementing new technologies to fully appreciate the extent of their costs over time, which likely include maintenance contracts. Table 5.8 provides sample comments.

Legacy Disposal

Although disposal of previous systems and equipment is a part of our conceptual model, we gleaned very little information of interest from the interviews. Four agencies noted that they keep a fair amount of old equipment, such as computers and radios. Data are converted when possible and, in some cases, may be maintained in or on their original source.

[7] Interviews with the chief of police on January 27, 2020, and the administrative captain on January 28, 2020, for two separate police departments in Southern California.

[8] Interviews with the system administrator on January 29, 2020, the chief of police on February 4, 2020, and the administrative lieutenant on February 7, 2020, for three separate police departments in Massachusetts.

[9] Interview with the chief of police for a police department in Massachusetts on February 4, 2020.

[10] Interview with the chief of police for a police department in Massachusetts on February 13, 2020.

[11] Interviews with the system administrator for a police department in Massachusetts on January 29, 2020.

[12] Interview with administrative lieutenant in charge of training, technology, and dispatch for a police department in Massachusetts, February 7, 2020.

[13] This came up explicitly in seven interviews with police departments from California and Massachusetts.

TABLE 5.7

Sample Comments on Purchasing

Interviewee, Organization, State, and Interview Month and Year	Comment
Chief of police, PD in Southern CA, January 2020	“Over $15 million means we need approval from city council before acquiring.”
Administrative captain, PD in Southern CA, January 2020	“The impediment is always money. ICI [ICI Systems, a regional radio network provider] is going to be a monthly fee per radio. Everyone around us is either already on ICI or going to ICI, so that’s why we are going that direction. ICI transition will be in the next year.”
Administrative captain, PD in Southern CA, January 2020	“For big projects, we have to go through the city council to ask for capital improvement funds. This can sometimes mean money is reallocated within an existing budget but could also happen through the city council setting up an account and putting money into the account for the project—so, finding money from somewhere else. The technology upgrades budget is going to have to increase in the future with the direction everything is going.”
Business manager, PD in Southern CA, January 2020	Q: “Is there information that is particularly useful in making [a] decision?” A: “Costs and where the money is coming from. Not every agency has budget to cover these things.”
System administrator, PD in Southern CA, January 2020	“[We] have to use a state contract; big technology stuff is all on statewide contracts. The state negotiates pricing with some vendors, and then all municipalities can buy on the contract. It’s not always the best price; if we get a better price from a vendor, we have to show that to justify to the state why we didn’t buy on the contract. [This is] sometimes done by vendor or type of equipment; for example, there was an IT software contract to buy from Dell. More information is available on the [state’s] procurement office website.”
Business services administrator, PD in Southern CA, January 2020	“The central IT department ends up making all of the purchases themselves, but they have liaisons in each department that understand their specific business needs.”
Business services administrator, PD in Southern CA, January 2020	“We use RFPs for the larger acquisitions; those also tend to involve a consultant. Sometimes a separate RFP is used for the consultant.”
IT personnel, sheriff’s department in Southern CA, January 2020	“We came up against an interesting challenge. We wanted to group purchases to get the most value out of [the] life cycle, but finance wanted us to trickle purchases instead of making big purchases—easier for finance to assure funds this way. Financial strategy doesn’t always result in the best purchasing strategy.”
IT manager, PD in Southern CA, January 2020	“We use the general budget—[it] generally has to be planned, and we can leverage funds from Measure A [people] and Measure P [infrastructure]—these are tax initiatives. Sometimes it’s from asset seizure, and then also grants. We look at the time schedules and the required compliance with the funding source to determine which source we will go after.”
IT manager, PD in Southern CA, January 2020	Q: “Do you have any tips or lessons learned you would like to share with other agencies?” A: “There is a new thing we just started under the smart cities initiative called challenge-based procurement—instead of doing the RFP, we put out the challenge. We’re currently targeting small startups that might have a data scientist. It’s a concern for me to execute. As for lessons learned, to be innovative to rapidly adapt, need to be able to take on risk. [This] can devolve the risk and mitigate through people, process, and technology.”
Chief of police, PD in MA, February 2020	“We try to use state contracts; [it’s] more efficient for us because we’re small.”
Head of technology, PD in MA, February 2020	“This is the red tape; [we] have to go through the purchasing department and get it approved by auditing. Then we can order it. It’s time consuming. We use the state contracts—purchasing handles this. If it’s not under state contracts, then we go through the bid process if it’s over a certain amount. Or we might do a sole source agreement—had to do that with the internal cameras—because of the need for interoperability.”
Chief of police, PD in MA, February 2020	“New RFPs were made, and purchases went through the state bid vendor list, which is much more convenient and simpler rather than trying to go through another vendor.”

NOTES: CA = California; MA = Massachusetts; PD = police department. City and agency names are withheld to protect interviewees’ anonymity.

TABLE 5.8
Sample Comments on Implementation and Maintenance

Interviewee, Organization, State, and Interview Month and Year	Comment
System administrator, PD in MA, January 2020	Q: “Radio maintenance contract?” A: “It’s about $16,000 a year. Reliable system. We have seen some improvements in technology, but there is still background noise; [it] can be hard to hear.”
System administrator, PD in MA, January 2020	“Hardest is probably implementation and maintenance for most agencies—[there is a] lack of technical skill and knowledge of how to communicate with vendors.”
IT manager, PD in Southern CA, January 2020	Q: “You do maintenance in house?” A: “We don’t do electronics repair; we buy the maintenance contract. [We’re] not staffed to handle this kind of repair—it’s a training and personnel issue.”
Chief of police, PD in MA, February 2020	“Our maintenance contract on radios is about $30K a year for emergencies and repair.”
Administrative LT, PD in MA, February 2020	“People forget you need to spend a lot on training when you implement something, and the need to retrain because you don’t use it all the time. Getting everyone trained is difficult because we can’t pull everyone in at the same time. Maintenance contracts can be really high—that’s where a lot of the vendors are making their profit.”
Head of technology, PD in MA, February 2020	“Ask about who is managing and storing the information; do we need a server? Try to have maintenance contracts on everything.”
Chief of police, PD in MA, February 2020	“. . . for example, body cams: several agencies have purchased them through grants but then have to put the program to bed because of the shear cost of data storage and records retention. Our CAD system maintenance contract is about $22K a year.”
Chief of police, PD in MA, February 2020	“Most will have maintenance contracts. $62K a year for maintenance for fire, police. $26K a year for updates.”

NOTES: CA = California; MA = Massachusetts; LT = lieutenant; PD = police department. City and agency names are withheld to protect interviewees’ anonymity.

CHAPTER SIX

Broadband Communications Costs for Law Enforcement Agencies

As a follow-up to the discussion of funding and acquisition in the previous chapter, we now focus on costs that law enforcement funding authorities should consider when budgeting for broadband communications. Besides the obvious costs associated with the procurement of mobile devices and the service plan fees for operating the devices, there are several other costs that require consideration (e.g., compatible routers to install in first responder vehicles) when developing a broadband communications budget. These can include nonrecurring costs associated with overseeing the fielding of wireless equipment and recurring costs to maintain the equipment.[1] Other initial nonrecurring costs might include labor to integrate mobile apps and back-end databases, such as CAD/RMS. There might also be an initial material cost for technology solutions to bridge LMR and broadband communications.

Specific recurring maintenance costs might include labor for managing the software and network administration of the software applications and data going across the broadband network. In addition, there might be recurring service fees for MDM and MAM software.

Some other cost considerations are labor and materials for training users of the hardware and software applications and costs associated with the development, procurement, and maintenance of mobile apps. In the following sections, we briefly discuss cost drivers, trends, and data, where available, for each of these cost elements.

Mobile Devices and Service Plans

We first discuss cost considerations specifically pertaining to the procurement of mobile devices utilizing broadband communications, such as smartphones and tablets, and the service plans required to use these devices. It is important to understand that most, but not all, police vehicles are equipped with mobile routers that serve to facilitate LMR/LTE connections between a unit and base stations and other users in the network. If an agency elects to contract with FirstNet, there are at least three FirstNet-compatible routers available for this purpose.[2] Although pricing for mobile devices and service plans will be similar to those advertised to the general public, it is likely that law enforcement agencies can leverage volume discounts or public entity–specific discounts to lower these costs. Individual agencies might want to explore whether they can increase

[1] All nonrecurring and recurring labor costs could be provided with in-house employees or through contracted support. These decisions would be based on an organization's size and available in-house IT expertise. Although this chapter does not provide guidance on whether these activities should be provided in house or outsourced, its intent is to inform decisionmakers about the types of activities and costs that their organizations must consider when adopting broadband communications.

[2] Cradlepoint (owned by Ericsson), Sierra Wireless, and Peplink routers are examples of available routers in FirstNet's app store.

possible volume discounts on the procurement of devices under larger blanket contracts (to include other state and local entities) rather than contracting on their own for a smaller number of devices for their agency.

Scenarios Specific to Law Enforcement

There are some scenarios specific to law enforcement in which budgeting for mobile devices and service plans might require some additional analysis. We explore the cost implications of scenarios in which agencies are reliant on a single network provider (e.g., FirstNet, Verizon, T-Mobile), use a dual-service option, or rely on a single provider while using an integrated LMR/LTE device.

Single Network Provider

In the single-provider option, the mobile device options are similar regardless of the network provider. Even FirstNet, the most restrictive network provider (which requires a device that is FirstNet ready), offers a multitude of mobile device options at price points ranging from just over $100 to the nearly $1,800 Samsung Galaxy Fold. In this scenario, budgeting for agency-purchased mobile devices simply requires determining the quantity of required devices and negotiating any possible discounts based on large quantities or government use discounts. As for service plans associated with the single-provider scenario, most vendors offer unlimited plans for each device or plans that allow various amounts of data to be purchased.

A further distinction related to FirstNet service plans is that they can be directly paid by the agency or employer, or by the employee. If the agency pays, there is an option to buy pooled data that allows purchased data amounts to be shared among multiple devices. FirstNet provides cost information for its service plans on its website (FirstNet, undated). Unlimited service plans range from $40 to $45 per device per month, regardless of whether they are paid for by the agency or by the employee, and include data, mobile hotspot, and tethering in all plans and unlimited talk and text in plans at the high end of the cost range. Purchasing plans that are not unlimited are posted on FirstNet's website; these include agency-paid pooled data plans ranging from $28.50 for 2 GB per month to $3,702 for 1,000 GB per month. Other vendors, such as Verizon, offer similarly priced service plans with discounts for first responders. Each agency should perform an analysis based on historic or expected data usage to determine whether unlimited plans or pooled data plans are more cost effective for the agency's specific range of anticipated uses.

Dual-Service Option

In the second scenario, agencies might wish to operate on more than one network, perhaps because of coverage issues associated with a single provider or for redundancy capability in the event that one network provider is overwhelmed in a particular area, resulting in service disruptions from that provider. The ability to operate on another provider's network helps maintain connectivity in such instances. Fortunately, this option is less costly from a device procurement perspective than it once was, since most modern mobile devices provide a dual-SIM capability that allows a user to operate on two networks on the same device by changing a SIM card or using a virtual eSIM, as is used in Apple devices. At most, the additional cost from a hardware perspective is the minimal cost of an additional SIM card in devices that require two physical SIM cards to operate on two networks. The costliest aspect in this scenario is the requirement to pay for two service plans. For instance, if an agency requires the ability to operate devices on both the FirstNet and Verizon networks, it would need to purchase service plans from both vendors for each device with that requirement, essentially doubling its service plan budget.

Single Provider with an Integrated LMR/LTE Device

In the final scenario, which has potentially large cost impacts from a device standpoint, agencies use an integrated LMR/LTE device, which enables the user to leverage broadband and LMR capabilities on the same device. There is even a touchscreen device on the market that provides LMR capability, the Motorola APX Next. Harris also manufactures an LMR/LTE device, the XL-200P, but it does not provide the touchscreen capability of the APX Next. Although the obvious benefit from a cost perspective is that agencies might be able to reduce their LMR expenditures by using an integrated device, it is not clear that agencies would be willing to make this change, and the cost of these new devices is quite high. The suggested retail price of the Motorola device is upward of $7,000, and the Harris device retails for about $3,000. These devices might be appropriate for very specific applications or job positions, but their high cost likely makes them suitable only for niche applications.

Managing the Cost to Field and Maintain Mobile Devices

We now turn to a discussion of the costs associated with managing a fleet of mobile devices, including procuring and fielding the devices and maintaining the fleet. The activities associated with this management include invoice processing; inventory control; billing errors; contract negotiations; data security; distribution of mobile applications; mobile policy compliance; and device maintenance, including management of spare parts, repairs, and replacement of lost or stolen devices (Harris and Romesburg, 2002; Imel and Hart, 2003; Salmensuu, 2019). These management services can be conducted in house by the agency (i.e., using its own dedicated staff), or the work can be outsourced to a third party.

Table 6.1 shows the average number of employees required as the number of devices managed increases. For illustrative purposes, if the full cost of a full-time equivalent (FTE) member of staff responsible to manage mobile devices is $200,000, it would cost $200,000 to manage 400 units and $1,000,000 to manage 3,500 units.[3]

Depending on the size of the agency procuring and managing mobile devices, it might be more cost effective to outsource this management to an external service provider. Outsourcing this work might be more cost effective, mainly because of the automation and expertise that a third party can have in the management of mobile devices.

TABLE 6.1
Average Number of In-House Employees Required for Device Management

Mobile Device Units	Employees Required
400	1
850	2
1,500	3
2,400	4
3,500	5

SOURCE: Mobile Solutions Services, 2014.

[3] The reader should not assume that an FTE is $200,000 for their specific case. This figure is used only as an example, for illustrative purposes. Each agency will need to use the appropriate FTE cost for its specific market. The full cost of an FTE includes the direct cost (e.g., salary and bonuses) and indirect cost (e.g., fringe benefits, such as health care and retirement). All costs associated with an FTE must be included when developing a budget.

Mobile Device Management and Mobile Application Management Service Fees

There are many types of mobile device services used by organizations to assist in the management of their mobile fleets. These services include management of the hardware (i.e., the mobile devices themselves) and management of the applications and associated data stored in the applications. In recent years, vendors have bundled these services into holistic packages that include management of both hardware and applications. Many providers offer various package options with more features and associated higher fees. In addition, there have been more vendor solutions to integrate and manage all organization IT equipment, including mobile and nonmobile hardware, software, and data. Organizations might prefer to choose one of these options to economize on costs and streamline IT management.

First, we will define some common terms used in the domain of mobile device hardware and software management: *MDM*, *MAM*, and *unified endpoint management* (UEM).

Mobile Device Management

MDM is a service that enables a mobile device to be tracked, managed, and secured through a profile specific to the employee using it and their tasks. MDM lets an organization provision and configure Wi-Fi access; install and manage enterprise applications, such as email; and address any problems that arise on a device. It also allows IT to enforce device security, such as locking a device and wiping data if the device is lost or an employee leaves the organization. In the bring-your-own-device model, whereby employees use their personal devices for work, many employees might be resistant to allowing employers to have the ability to track, manage, and access data on their mobile devices, particularly when they are also for personal use and contain personal data. Before acquiring MDM software services, however, the organization should accurately assess the number of devices and frequency of usage to avoid overinvesting in MDM licenses and lower levels of use of these services.

Mobile Application Management

MAM is a service that is more targeted than MDM, focusing solely on enterprise applications and the data associated with them, not the devices themselves. The most common application managed by an organization is the organization's email, but this service can manage all types of applications that have data that require protection from spillage to public applications. MAM can include collaboration tools and applications that contain data that law enforcement might wish to protect or that require protection because of laws and regulations. MAM allows IT to control applications that hold sensitive data, while allowing personal data on the device to remain intact if an employee loses the device or leaves the organization. MAM also allows applications to be remotely updated with new features and patches, making it relatively easy to address new security threats quickly.

Unified Endpoint Management

Some organizations might use enterprise IT solutions that include MDM or MAM services, or both, and therefore do not require separate considerations for MDM and MAM services. This type of IT solution is likely more applicable to larger organizations that require management of a large IT portfolio. This approach, which is often referred to as UEM, allows an IT department to remotely provision, control, and secure everything from cell phones to tablets, laptops, desktops, and Internet of Things (IoT) devices. UEM can manage devices across a variety of platforms, at least theoretically, making it easier to lock down hardware and protect critical data.

Costs Associated with Different Options

Given the various services that a vendor can provide, including MDM, MAM, and UEM, costs can vary dramatically. As noted, many vendors offer some combination of these services and various price points. The types of services provided are the largest cost driver determining service fees. A 2018 study by Oxford Economics found that organizations are spending between $3.25 and $9.00 per device each month for MDM and MAM services (Oxford Economics, 2018). Our research into publicly available pricing on vendor websites suggests that this range is a reasonable estimate, although we found some vendors that offer very basic plans for less than $2 per device each month.

Given this rather wide range in monthly cost, it became evident as we researched vendor websites that there are several parameters affecting cost beyond just the number of services or features associated with the plan. First, several vendors show how the number of devices that an organization is managing can change the pricing schedule for fees. Unsurprisingly, economies of scale are realized and reflected in pricing as more devices are added to reduce the fee per device. For example, one vendor's monthly per-device fee was as much as 70 percent less for managing a handful of devices (25 or less) than for managing 10,000 devices or more.

Another common cost driver, although not a significantly large one, is related to how the organization is billed and pays for the service, specifically the frequency of payment. In most cases, vendors provided discounts to organizations paying fees on an annual basis versus monthly. This is a common practice for any service fee–based pricing model because it reduces risk for the vendor and stabilizes revenues over a longer period. At least one vendor required an annual commitment. Another vendor offered a perpetual service fee with a significant discount for organizations that are confident that they would be comfortable with the lock-in cost to use the same vendor for an indefinite period. If after a short period the organization wished to use another vendor, the initial higher cost of a perpetual license would have been a poor investment.

The management and storage of data was another option noted by some vendors that affects cost. Some vendors had options for on-premises or cloud-based data management. One vendor that quoted these price differences on its public website showed a 30-percent premium for cloud-based data management relative to the on-premises–based service.

Another pricing model distinction that varied by vendor was that some vendors' fees were on a per-user basis instead of a per-device basis. In all cases, the per-user fees were higher. Services priced on a per-user basis were more common for the more robust UEM services that manage multiple devices being used by a single user. Unsurprisingly, per-user pricing models had a significantly higher cost per month; costs generally ranged from $10 to $15 per user per month.

Observations on Working with Vendors

We made some other useful observations after researching vendor pricing. Some vendors offered free basic services for managing small numbers of devices, usually from three to 25 devices. Almost all vendors offered, at minimum, monthlong free trials of their services. For organizations that are unsure of the best MDM, MAM, or UEM solution, it might be worth testing various vendors on a trial basis before committing to a vendor, especially on an annual or perpetual basis. Another observation was that while most vendors offered services that were hardware or operating system agnostic, there was at least one vendor on our list that provided services for only Apple devices and operating systems. While this vendor might be a good choice for an organization that uses only Apple products, because the services would be optimized for Apple, it would not be a good choice for an organization that requires service across multiple device brands and operating systems. This is especially true if the organization uses a bring-your-own-device model in which each user can choose whether to use an iOS phone or an Android phone. Finally, although this section is meant to help guide an organization's expected costs for MDM, MAM, or UEM services, all of the vendors noted that they should be contacted for specific pricing. Each organization's situation is unique, and, although all of the factors noted in this section will likely affect costs, the ultimate service fees will likely be negotiable with vendors.

Mobile Application Development, Procurement, and Maintenance

Another cost that an organization will need to consider in its mobile device budget is the cost of development or procurement of mobile apps in support of its mission. In addition, there will be a maintenance cost associated with any apps developed or procured.

Of course, many apps used will likely be existing apps that have already been developed; however, depending on the agency's needs, they might also be new software developments (or at least customizations of existing software that require new coding), which require budgeting for their full life cycles (i.e., development, testing, implementation, and maintenance).

For existing apps, some will be free to users, but some might have associated fees. Fees can be one-time, per-user fees or recurring fees (e.g., monthly or annually). Budgeting for existing app fees simply requires the number of estimated users of an app and the fees for the app, whether they are recurring or nonrecurring.

Costs increase if an organization requires modification to an existing app or a completely new custom app. While this report does not provide an entire discussion of app development considerations, since there are too many factors to consider, it does note some key aspects and potential hidden costs that an organization will need to take into account if it is embarking on a custom app development effort. One source notes that the cost of developing an app can range from $60,000 to $300,000 per platform (e.g., iOS and Android) (Lastovetska, 2022). Some of the key cost drivers in app development are vendor type and location, app complexity and number of features, back-end infrastructure and connected application programming interfaces, complexity of user experience (UX) and user interface (UI) design, development approach (e.g., native, mobile web, hybrid), and number of platforms to be developed. In addition to the actual coding of the app, there are other life-cycle costs that will need to be captured in the total cost of the app, including design, back-end development, security, architecture, testing, and maintenance.

Another source discusses some of the hidden costs of app development (Matyunina, 2021). Broadly speaking, these costs fall into four categories: functional, administration, infrastructure, and IT support. Functional costs are associated with implementing certain functionalities, which might require subscriptions to services for delivery mechanisms, such as integrating SMS messages or email into mobile apps or push notification services. Administration costs are costs for such items as content management tools, dashboard emulators, functional services management, dynamic updates, analytics, access controls, and data segmentation. Infrastructure costs include app hosting, data storage, and data delivery fees. Finally, IT support costs are mostly related to maintaining the apps and can include costs for app update submissions, iOS and Android updates, maintenance of application programming interfaces, and bug fixes.

Regarding app maintenance costs, there are several specific activities to consider. App maintenance costs include costs for updates to maintain compatibility with mobile device hardware and operating system software upgrades, upgrades to UX and UI to align with current trends, upgrades to or addition of new features, recurring app hosting fees, and identification and fixing of bugs. Although maintenance fees can vary depending on the specific application, several sources suggest that a good rule of thumb for app maintenance costs is 20 percent of the initial development cost annually. Therefore, if an organization's app cost $100,000 to build, the organization should expect to pay $20,000 annually to maintain the app.

Back-End Infrastructure Integration

Finally, there can be costs associated with integrating mobile devices and applications with back-end infrastructure, such as CAD/RMS database systems. Depending on the vendor, CAD/RMS mobile connections might be included as part of application deployment agreements; however, these connections might not be included, and some could require custom interface development, the cost of which might not be trivial. Agencies might want to be aware of these potential costs and be prepared to budget for labor expenses to integrate mobile apps and back-end databases. In addition to the nonrecurring cost to develop the interface, there will be a need to maintain it as required by the vendor to update apps or the databases with which they interface. This report does not provide cost data for CAD/RMS integration, because each agency scenario will be quite specific and the effort and costs will depend on the particulars associated with each scenario. It is important for agencies to be aware that these potential costs might be part of their broadband communications budgets.

There can also be acquisition and maintenance costs for technology solutions to bridge LMR and broadband communications. There are three general technology solutions to bridge LMR and broadband: IP solutions, hardware gateways, and dual-mode radios. This report does not provide cost data for the bridging solutions. As noted in Chapter Three, IP solutions are the most time consuming and costliest to implement. The gateway solution might be a relatively affordable option for bridging LMR and LTE, as NIST has recently developed and demoed a prototype that promises to be a low-cost solution for budget-constrained agencies (NIST, 2021). Unfortunately, NIST has not yet provided cost data.

CHAPTER SEVEN

Barriers and Issues

So far, this report has focused on strategies and considerations to assist agencies in moving forward with broadband communications acquisition. However, it is also important to be aware of key barriers and other issues that could impede progress to the desired end point.

There are three primary barriers to the movement from any status quo state to an envisioned interoperable public safety broadband platform from which to conduct police and related public safety functions. To optimize the use of the NPSBN or an alternative broadband system for an agency and community, these considerations are necessary building blocks from which to make informed decisions about the infrastructure, management, and deployment of any system:

- **Governance.** How will any future LMR/LTE interoperable system be managed? Should an agency "go it alone" to acquire devices and contracted broadband capabilities, or should agencies in any particular region consider how broadband must work seamlessly with LMR systems to transmit voice, data, and related communications? There are existing joint-powers agreement consortia for LMR and LTE broadband that can help agencies understand the advantages of consolidated management of any future system, although there will be significant work to create such governance if an existing structure for dispatching, records management, or other regional cooperatives does not already exist.
- **Functionality.** The federal government established the NPSBN and created FirstNet as an envisioned universal platform for all public safety broadband needs and then contracted with AT&T to build and operate that network under the management of the FirstNet Authority Board. As states agreed to join FirstNet and cooperate with the development and deployment of the network, other broadband providers created similar networks and infrastructure to compete for police, fire, and EMS business. This has caused considerable confusion for end users as they make choices with regard to their systems, devices, and inevitable trade-offs of cost versus coverage. Beyond any confusion, decisionmakers want to focus on three functionality issues: system reliability, system coverage, and system survivability.
- **Confusion.** There are many mobile broadband labels, including 3G, 4G, 4G LTE, 5G Evolution (5G E), 5G Ultra, 6G, MCPTT, and Z-Axis. There are 2,784 internet providers in the United States, nine of which serve more than 100 million people. Of those providers, there are 464 cable companies and 1,685 fixed wireless broadband providers (BroadbandNow, undated). Each of these companies is vying to retain or grow its market share, and many have existing contracts with public safety entities that they wish to continue.

At the same time, FirstNet was created by the federal government, which facilitated a process to select AT&T to deploy the system for the benefit of the police and others to resolve issues with interoperability and emergency communications. The net result of all of these factors is that many law enforcement leaders are confused by the claims and options. Many interviewees expressed confusion, as well as fatigue from vendors repeatedly contacting them to try to persuade them to retain their current broadband providers, switch to public safety–tailored platforms, or transition to FirstNet.

We discuss these barriers in more detail in the following sections. In addition, we describe other issues and challenges identified through interviews.

Governance

There are about 18,000 law enforcement agencies in the United States at the local, state, tribal, and federal levels. Each of them uses some form of LMR network for voice communications, and each has a methodology to capture and collect data for local, state, and the federal National Incident-Based Reporting System (NIBRS). It is not uncommon for police agencies to have independent CAD/RMS to facilitate the intake of calls for police service, to facilitate the dispatch of officers, and then to document and store police reports. Many agencies have also integrated mobile broadband services into their array of communications options. Others use mobile devices (e.g., smartphones and similar devices) more informally, either buying them for all or some staff or allowing officers to use their own smartphones for duty.

The flexibility of tailoring an approach to a particular agency is a strength of a decentralized policing approach; it is also a hindrance when the ultimate goal is interconnecting police resources and deploying a seamless interoperable network of communications that can talk and share data across agencies and platforms.

To resolve issues with regard to governance, the creation or modification of a joint-powers agreement or similar shared governance model can be considered. Developing a contract and a formal board of directors to guide the purchase, use, and expansion decisions would deconflict issues that result from fragmented purchasing processes or incompatible equipment, frequencies, or technology platforms. It would also result in the development or sustainment of interagency cooperation at the administrative level to resolve conflicts for all aspects of first responder communications.

Functionality

For the end user, functionality is the overriding concern, as evidenced by the issues that resulted in the congressional action that created the NPSBN and as noted in almost every interview with users. Ostensibly, the development of FirstNet resolves that issue, and other broadband providers would not be competitive as FirstNet's platform, technologies, and applications came to market. Even though the NPSBN was allocated Band 14 for exclusive use by first responders, no prohibition was placed on providers who did not respond to the RFP that resulted in FirstNet contracting with AT&T. This means that other broadband providers who might have been providing broadband communications services to agencies could continue to do so until these agencies chose to transition to FirstNet (or not).

As previously discussed, Verizon created a public safety slate of services that was intended to retain its market share and solicit new business, and, more recently, T-Mobile began marketing first responder preferential contracting and service. Although any commercial broadband provider is within its rights to market its communications technologies to law enforcement and the first responder community, it can also create substantial confusion as decisionmakers are faced with claims that sound similar, functionality that appears to be essentially the same (such as priority and preemption), and opaqueness about the actual meanings of such terms as *public safety–grade* when they are used by FirstNet or others.

Because FirstNet and commercial providers do not publicly provide specific data or information on the capabilities of their platforms, individual agencies or joint-powers authorities must ensure that whoever they are considering for first responder broadband service has an appropriate bandwidth; adequate functionality for routine, emergency, and large-scale or disaster needs; and sufficient coverage for mobile broadband to address both current and future needs.

These considerations should include ways in which the system interacts with LMR; the system's interoperability with other segments of government, both within a jurisdiction and for interjurisdictional needs; planned additions to coverage and capabilities, as articulated in a contract for services; the presence and use of public safety–grade hardware; and the functionality of MCPTT and preemption of bandwidth for law enforcement and other first responders. A final consideration is that any LMR/LTE mobile communications system that transmits, generates, stores, or receives criminal justice information must conform to the requirements of the FBI's *Criminal Justice Information Services (CJIS) Security Policy* for MDM and wireless device risk mitigation.[1]

Confusion

All end users have existing investments in devices and systems for their LMR/LTE functionality, including contracts for broadband service. During a time of transition to FirstNet or another system, there will be potential issues with LMR/LTE integration, legacy devices that might or might not be compatible with a future broadband platform, and the need for added work to develop a multi-jurisdictional interoperable platform from which police and other public safety functions can interact. Expenses should be anticipated for contracted services, physical devices for mobile users, hardware and software infrastructure development or modification, and personnel time to manage and complete the necessary work to create a successful outcome.

There are several sources of possible confusion for law enforcement leaders as they consider the acquisition of new public safety broadband platforms. The following are among the most significant:

- The NPSBN and FirstNet are readily recognized and known by agency representatives whom we interviewed. Interviewees said that AT&T/FirstNet.com representatives arrived on a recurring basis to solicit their subscriptions to the FirstNet platform, and many interviewees said that this was "too much" in terms of feeling pressured to sign up. The nature of the sales pitches that they repeatedly received led some interviewees to think of FirstNet less positively. A challenge for end users is to separate FirstNet.gov; the FirstNet Authority Board created to manage the implementation of the NPSBN and enforce compliance with the FirstNet contract; and FirstNet.com, AT&T's deployed platform.
- Another area of confusion is the necessity of the deployment of 5G as a precondition to the transition to FirstNet. Although AT&T recently committed to integrating 5G technologies into the FirstNet platform, some interviewees misperceived that development as meaning that either the capabilities of 5G would make FirstNet a singular option or 5G would enable FirstNet to deploy significantly better service to public safety, thus making the decision to transition to FirstNet as a primary broadband service an easy one.
- The confusion over capabilities, both present and future, is more difficult; commercial providers, including AT&T/FirstNet.com, do not publicly state the specifics of their coverage or capabilities because of those data being a source from which their competitors could seek an advantage (because AT&T's data could disclose the presence of intellectual property of a provider of which competitors might not be aware). Although these are rational positions taken by broadband providers and suppli-

[1] See Criminal Justice Information Services Information Security Officer, 2020, Sections 5.13.2 and 5.13.3, respectively, for the specific requirements for mobile communications platforms and services.

ers, they decrease a decisionmaker's ability to compare "apples to apples" in terms of cost, coverage, and reliability of a proposed or envisioned system.

- Broadband providers, especially those with current contracts for public safety broadband, offer public safety platforms with many of the same, or similar, features as those of FirstNet (e.g., MCPTT, prioritization and preemption) and assert that their platforms are essentially comparable to that of FirstNet. It is true that FirstNet's competitors offer similar capabilities, although none of them are a result of the governmentally created and managed process that was used to create FirstNet, so the functionality and reliability of public safety broadband providers that are not FirstNet would be contractual issues between these providers and their customers.
- Many interviewees mentioned that they knew they would have to transition to FirstNet "at some point" but were unclear as to what functionality would prompt a decision to change or at what point the decision could be made. Every interviewee said that coverage was a decisive factor in the decision. Several also said that they had contracted with FirstNet (or with Verizon or comparable platforms if they were AT&T/FirstNet clients) to have redundancy in coverage in case one platform failed to perform in an emergency.

Most interviewees, except for those who were already members in a regional governance consortium, such as a joint-powers agreement, did not give high priority to two factors that we consider crucial for a future broadband deployment to succeed: (1) effective governance of the platform to provide regional cooperation and interoperability and (2) public safety–grade base stations, towers, and mobile devices. The absence of these strategic "bright lines" deflects a sense of urgency to change. It might also mean that a singular focus on coverage could result in decisions to expend funds without considering the development ecosystem within which public safety broadband exists.

Other Issues and Challenges: Voices from the Field

In interviews with end users and other stakeholders working to create the future of mobile broadband for their law enforcement and first responder organizations, there were many comments that are relevant to the themes and issues being experienced nationally. We include them in this section so that agency personnel understand that (1) they are not alone; (2) there are no easy answers; (3) any progressive change requires hard work, expertise, and persistence; and (4) the universality of issues means that there are solutions and best-practice choices that can be applied nationally. The comments are intended both to help agencies understand the shared perspectives that they might have in common with the interviewees and to illustrate the difficulty of transforming a vision of the future into a functional reality for end-user law enforcement and first responder personnel.

Issues noted fall into four general categories: acquisition and management of systems (including costs), the regulatory environment, personnel staffing and usage, and the realities of coverage for devices and organizations.

Acquisition and Management of Systems

There were several concerns with regard to paying for new systems, optimizing sunk costs in existing systems during a transition from old to new broadband platforms, and prioritizing infrastructure expenses during a time when a jurisdiction might be experiencing declining revenues or increased costs for other aspects of the organization. The following are some comments not captured elsewhere in this report:

- "With acquisition, the legal folks are heavily involved with everything. Three full-time county attorneys are assigned to the sheriff. The vendors get frustrated with this—it can extend [the] process months."[2]
- "City went bankrupt, so we had to stop, and then we are slowly adding things back."[3]
- "We put the program to bed because of the sheer cost of data storage and records retention."[4]

The Regulatory Environment

The regulatory environment, both for broadband use by public safety and for the police in general, shifts constantly, and end users often struggle to keep up with new mandates, obligations to report data, and solutions to optimize these requirements. California's RIPA is one example of a statewide law that requires substantial modifications to what the police report, the new data that must be retained and reported, and the ways that technology (including broadband) might support it or be an obstacle to implementation unless systems conform to regulatory requirements. This reluctance results in end users choosing to refrain from acquiring devices or initiating new services. The following are some comments not captured elsewhere in this report:

- "We have to issue every cop a phone to comply with RIPA."[5]
- "RIPA-compliant through the RMS—we piloted it, but it's hard for officers. NIBRS is also changing things for RMS."[6]
- "Currently, only detective or sergeant and above get department-issued phones. If CAD/RMS was more friendly on the phones, we would give all officers phones."[7]
- "[We're] not going to go to mobile CAD-RMS given Cal-DOJ compliance. It's too hard to get phones as MDT at the moment."[8]
- "We have looked into cloud storage, but there's currently no Cal-DOJ–compliant service because you have to know the location of your data."[9]
- "[There is] potential for down the road there being federal requirements to move off the band we are on, which is UHF high. There is a rumor there is legislation coming down. This would be a huge cost to the communities."[10]

We understand that additional legislative changes or mandates can affect law enforcement use of technology and subsequently have budgetary and training impacts. For example, from May 2020 to April 2021, six states passed laws governing police body-worn camera use. In some cases, grants or bonds have been authorized to defray program costs (Wagner, 2021), but the short- and long-term impacts of the programs might still pose difficulties in terms of costs and staffing. Furthermore, these mandates could affect adoption or prioritization of the mandated technologies over other technology.

[2] Interview with a captain at a sheriff's department in Southern California on January 30, 2020.

[3] Interview with the IT liaison at a police department in Southern California on January 30, 2020.

[4] Interview with the chief of police for a department in Massachusetts on February 19, 2020.

[5] Interview with the chief of police for a police department in Southern California on January 27, 2020.

[6] Interview with the business manager for a police department in Southern California on January 28, 2020.

[7] Interview with the business services administrator for a police department in Southern California on January 29, 2020.

[8] Interview with administrative personnel for a police department in Southern California on January 29, 2020.

[9] Interview with administrative personnel for a police department in Southern California on January 29, 2020.

[10] Interview with the chief of police for a police department in Massachusetts on February 19, 2020.

Personnel Staffing and Usage

The most expensive item in any police budget is that for the people who work in the organization. Personnel costs can account for more than 80 percent of an agency's total budget, meaning that cuts to an overall budget will almost certainly involve reducing positions and, unless a broadband solution is user friendly, the assets created for police use will lay untouched. Considerations in this category also include training time for users to become accustomed to new systems or functionality and the generational realities of newer, more tech friendly employees. Comments related to personnel and staffing included the following:

- "We are struggling to hire IT people because of money; we can't attract good talent here."[11]
- "The younger generation like the digital system. Older officers were fine with paper tickets but the younger officers said, 'No, don't go back to paper tickets.' Big generational shift in law enforcement."[12]
- "With the younger generation, they would rather text than make a phone call. They will text a sergeant a question instead of radio."[13]
- "We are struggling to hire cops, struggling to hire dispatch. Stay long enough to get trained and then go to other places that can pay better."[14]
- "Cops don't like change, so personnel has been the biggest challenge. They want to know, 'Are we going to get paid for training?'"[15]
- "[It] will probably be easier for younger, tech-savvy officers to acclimate to and a struggle for older officers to learn a new system."[16]

The Realities of Coverage for Devices and Organizations

The most prevalent comment made by interviewees was that they were less concerned with who provided a broadband network than with whether it provided appropriate coverage for their first responders in all circumstances. The "I just want to be heard when I press the button" sentiment was pervasive and a factor in any decision to either transition to FirstNet or remain status quo until solutions achieved a consistent level of coverage that was at least as good as current systems. The following were among comments related to this issue:

- "We are still waiting to see what they put in place—wireless routers, not knowing what CAD RMS. We don't know what functionality we need. A lot of demos we are seeing are integrated with smartphones and tablets; that's where the future is going."[17]
- "Probably better to be a centralized IT department; that way, resources can be moved around."[18]
- "When we want to stand up a new feature, it will almost always not work with us because we have to work with IT because of firewalls."[19]

[11] Interview with administrative and IT personnel for a sheriff's department in Southern California on January 30, 2020.

[12] Interview with the chief of police for a police department in Southern California on January 27, 2020.

[13] Interview with the administrative captain for a police department in Southern California on January 28, 2020.

[14] Interview with administrative and IT personnel for a sheriff's department in Southern California on January 30, 2020.

[15] Interview with the chief of police for a police department in Massachusetts on February 19, 2020.

[16] Interview with the chief of police for a police department in Massachusetts on February 13, 2020.

[17] Interview with the business manager for a police department in Southern California on January 28, 2020.

[18] Interview with the IT liaison at a police department in Southern California on January 30, 2020.

[19] Interview with the IT manager and chief of innovation for a police department in Southern California on January 31, 2020.

- "In a perfect world, everything would be done on a single device—doesn't have to be a phone, but should be able to access all systems, for example GIS [geographic information system] and radio."[20]
- "There is the red tape; we have to go through a purchasing department."[21]
- "We are hesitant to move regular police data to AT&T because of lack of coverage. Coverage is an issue even with Verizon in some schools, for example."[22]
- "We would really like to be able to push video. This will give us situational awareness for the officers on patrol and the communications center. Supervisors may not have to respond to a location because they can see what's going on. Go back and look at the video. We haven't done this yet because of the dependability of cell service; it's important not just for pushing information but for detectives that are running operations."[23]
- "Our biggest challenge is our cellular network. Sometimes we lose connectivity with MDT because those are reliant on cell service. They are limited to geographic areas—there is a lack of cell towers in those areas."[24]

As law enforcement executives, their technical staff, and broadband providers (including FirstNet) work to achieve success in the implementation of the NPSBN, it is important to remember that any systems (including legacy systems being retained for now) are costly and take time and energy and that real people engaged in critical first responder calls for service rely on them for their lives. The best solutions will be made when the users are not only considered but have their voices and experiences inform the decisions made on their behalf.

A common refrain is that mobile broadband devices will displace the "police radio"[25] in the foreseeable future. The outcomes of the coverage modeling (presented in Appendix B) strongly indicate that this perspective is not supported by the data. Although broadband offers advantages in one-to-one communications and the transmission of voice and data over shorter distances, the reliable connectivity of communications among devices and base stations will be best achieved through a platform that uses the advantages of both LMR and LTE/5G in a seamless and integrated fashion. There are, however, signs that some policing agencies might work to transition away from legacy LMR systems and use PTT as a mission-critical alternative for voice communications. In this approach, agencies would shutter LMR systems reaching end-of-life status instead of investing significant funds to modernize such systems (Jackson and Castillo, 2022). Even those testing this approach note that it is only a possible option and that the individual needs of agencies might dictate a continuance of LMR for critical communications.

[20] Interview with the head of technology for a police department in Massachusetts on February 7, 2020.

[21] Interview with the head of technology for a police department in Massachusetts on February 7, 2020.

[22] Interview with the business services administrator for a police department in Southern California on April 29, 2019.

[23] Interview with the chief of police for a police department in Massachusetts on February 4, 2020.

[24] Interview with the chief of police for a police department in Massachusetts on February 4, 2020.

[25] Here, we are referring to the traditional concept of a police radio (as opposed to hybrids or the more advanced multiband interoperable devices).

CHAPTER EIGHT

Conclusions and Key Takeaways

For a public safety executive, technology manager, or decisionmaker charged with assessing LMRs, broadband systems, and the future of the PSBN, the task to identify a specific best practice for an individual agency can be daunting. There are many critical questions to be answered, including the following:

- Are commercially available broadband network options sufficient for my agency and community?
- Is a transition to a public safety–specific platform both necessary and functionally advantageous?
- Should I adopt the federally sponsored PSBN being built by FirstNet.com and AT&T under the authority of the FirstNet Authority as per a U.S. Department of Commerce contract, or should I consider other options from competing vendors?
- Are such functions as priority and preemption, MCPTT, and LMR/LTE interoperability worth the time, effort, and money needed to integrate them into my agency's capabilities?
- If I think it is appropriate to transition to a police or public safety–specific broadband network, should I do it now or wait until 5G technologies and coverage are widely available?
- How do I work with other public safety organizations in my region, and are there advantages to coordinating efforts to save time or money?
- Is LMR going away and being replaced by broadband communications, or will it still exist even when the NPSBN is fully adopted? Why can't LMR just handle the communications needs for my officers and staff?

Key Considerations

There are four key considerations of which decisionmakers should be acutely aware during the acquisition phase, in daily and emergency use, and as ways to manage any system are contemplated: system reliability, system survivability, system upgradability, and system governance.

System Reliability

When officers, firefighters, or paramedics push buttons on their mobile devices, do the persons with whom they intend to communicate hear them? Is the coverage for such devices adequate, or are there gaps in coverage that could threaten lives or safety in an emergency? What metrics of reliability should be used to gauge an acceptable level of service for various needs and circumstances? FirstNet and others might say that their approaches are the best technology and configuration to ensure usefulness and survivability, yet different technologies might present differing advantages.

A critical aspect of reliability is the ability of a communications systems to interoperate smoothly with other systems. The congressional action that created the NPSBN did so to enhance the ability of police, fire, and EMS personnel to talk to one another in a prioritized, uninterrupted manner across agencies and disciplines. Technologies already exist to allow for cross-agency or cross-discipline communications via LMR or LTE. Rather than presuming that one platform can "talk" with others or relying on patchwork solutions (such as dual SIM cards in selected devices), agencies should determine the present and future reliability of proposed systems, both now and in the future, at the time that a technology provider is selected.

System Survivability

The NPSBN seeks to be "public safety grade" and should be able to survive the various natural and human threats to survivability, including wildfires; active shooter events; multiagency responses saturating networks; and weather events, such as hurricanes, tornadoes, intense rainfall, and earthquakes. The FirstNet Authority states that its cell towers and equipment are "Public Safety Grade" (Seybold, 2017b), although there is no standardized definition of what that means. In 2014, the National Public Safety Telecommunications Council (NPSTC) provided guidance to FirstNet to define *public safety grade* to refer to performance specifications and best practices necessary for mission-critical public safety operations (NPSTC, 2014). They noted that a public safety–grade communications system should be designed to "resist failures due to manmade or natural events as much as practical" (NPSTC, 2014, p. 3). Depending on the geography, topography, and recurring vulnerability to weather phenomena, agencies might already know the most likely and foreseeable threats to their broadband infrastructure. Any system that is employed for public safety broadband communications should be oriented to survive in those circumstances and to survive any novel threats that might emerge, as well as known recurring threats, such as wildfires, hurricanes, tornadoes, or other severe weather events that occur cyclically. As noted in the use case scenarios, planners must consider survivability in such instances as active shooter or mass casualty events, multiagency responses saturating network coverage capabilities, earthquakes, and similar unplanned events that could cause a system to fail in its functions.

System Upgradability

As discussed in Chapter Three, broadband technology has been evolving rapidly—and so have new devices, sensors, and applications that need ever more communications bandwidth. It is therefore important that agencies acquire broadband communications systems in ways that allow for relatively easy and inexpensive upgrading later, as technologies and demands advance, as opposed to having to pay the expensive, long-term costs of building new networks.[1] There are two aspects of upgradability that should be considered:

- Hardware: Are the devices that are being used (e.g., phones, radios) upgradable to new communications standards via software? Can the hardware be easily replaced or refurbished at the end of its life cycle, especially when new communications standards requirements outstrip the capabilities of the hardware to upgrade to them?
- Communications bandwidth: Especially for commercial bandwidth procurements, are the contracts written in such a way as to permit bandwidth usage upgrades as needed—or at least at reasonably small regular intervals, such as annually—or is the agency locked into a fixed communications capacity? The latter should be avoided.

System Governance

Although agencies traditionally manage broadband contracting, equipment, and deployment individually, the nature of an increasingly connected world might mean that economies of scale, interoperability issues, and policy conformance to ensure best practice standards would be better served within the structure of a

[1] See, for example, McHugh, 2022.

joint-powers agreement, a consortium dedicated to broadband communications capabilities (as more commonly exist for LMR) or a similar governance structure. In addition, FirstNet/AT&T, Verizon, and others might state that their technology and broadband platforms are the best means by which to ensure desired outcomes for public safety, yet they are on differing broadcast bands, use different equipment, and offer similar capabilities.

The specific capabilities of commercial entities are considered intellectual property. Disclosing these capabilities publicly can give an entity's competitors an advantage as they seek to grow or retain market share. Although this reluctance is understandable, it means that law enforcement agencies must ask for clear, specific details before they contract for service. Those details should include coverage capabilities (present and planned); system survivability; system adaptability, especially to incorporate desired functionalities or public safety applications; and performance metrics that agencies can use to gauge compliance with any contracted services.

Governance issues can also relate to political issues associated with the transmission and use of body-worn camera footage and the use of surveillance and tracking software systems that employ artificially intelligent capabilities to reduce response times, generate leads, view and analyze closed-circuit television and other camera footage to identify persons suspected of crime, and scan social media and offender registries to advise the police of crime and suspect data.[2]

Key Questions

When considering a transition to the NPSBN or another broadband platform, it is essential that decisionmakers choose their path forward knowing the specifics of the proposed technology and how it will perform in the real world. Advertisements, sales calls, and presentations rarely contain enough data and information from which to make a multimillion-dollar decision about software, hardware, and contracted services. It is incumbent on the agency seeking those elements of its communications platform to act only when it has articulated the specific performance, support, and development of whatever choice its decisionmakers make. With regard to broadband for law enforcement, several key questions should be asked of staff, potential vendors, and technology consultants that might be contracted for LMR or LTE. Among these are the following:

- What are the actual costs per device to integrate the new system into the existing one?
- What purchase requirements exist to acquire or lease necessary devices, infrastructure, or software services for the communications ecosystem in my agency?
- How will public safety broadband interact with my present and planned LMR systems? Will the encryption of police LMR interfere with interoperability?
- How do we best achieve economies of scale for our agency, the various public safety disciplines serving the community, and regional partners upon whom we will rely for large-scale incidents?
- What protections does the system have to ensure that it is survivable under the challenging conditions of a disaster or major event?
- What are the sunk costs to acquire and deploy a broadband system, and what are the recurring costs to maintain and improve it over time? Does the system support ready and inexpensive upgrades over time?

[2] There are systems that are already available for these purposes. In Utah, an agency was considering using an artificial intelligence–assisted system ("Utah Police Look to Artificial Intelligence for Assistance," 2020). Concerns about the use of artificial intelligence in social media appear in Fussell, 2021.

Final Thoughts

As Albert Einstein once said, "imagination is more important than knowledge, because knowledge is limited, and imagination encircles the world."[3] When thinking about the future, rather than merely following guidelines or considerations to create a new broadband infrastructure, it is more useful to imagine what the future might look like and how the issue that one is considering may have evolved since the present—e.g., how the world might be different when the envisioned and planned systems come online. To that end, we present "Broadband 2042: A Story of the Future," in which we envision policing and the impact of broadband technologies in 20 years. It is important to understand that this story is not a prediction of what will happen, but it does rely on current trends, events, and developments as a foundation for a possible future that decision-makers can think about while choosing next steps. Actions taken today will create the possibilities for future realities, so a useful first step is to imagine what the future might look like once we arrive.

Broadband 2042: A Story of the Future

Policing in 2042 is different from policing in 2022 in profound ways. The civil unrest and calls for change in the 2020s resulted in greater transparency for any and all police encounters. Mental health professionals largely take the place of cops on the street for subcritical mental health issues, offloading from the police a substantial call volume for which they were ill trained. Today's officers are supported in physical, virtual, and technological ways their predecessors could scarcely have imagined. Real-time analytics, scene awareness, and officer and community safety have changed dramatically, in large part because of the connected world—the IoT links early-warning systems to one another, and intelligent roadways and vehicular autonomy have resulted in thousands of lives saved. The frequency of severe weather events has repeatedly tested the limits of public safety infrastructure, from the survival of repeaters and cell sites to legislated restrictions on the use of artificial intelligence to scan social media and access surveillance data. However, one constant remains: The police need to talk with one another, share data, and know where to respond to resolve the endless series of human crises for which law enforcement's presence is the best option. In this sense, the new ways of 2042—officers and deputies interacting with mobile devices to share needed information and fulfill their mandate to protect the public—would be familiar to their predecessors in 2022.

In 2042, law enforcement communications are facilitated through a network where officers, firefighters, and medics each have a device that intuitively knows to whom the user wants to communicate and makes that communication seamlessly. The technological platform is a blend of leading-edge broadband communications platforms, including 5G and 6G capabilities to allow for ubiquitous unit identity, location, and *z*-axis information. "Comms tech" also includes LMR use, especially for one-to-many communications, contact across larger physical spaces, and quick dissemination of voice information. Most data are transmitted via routers embedded inside handheld devices. Public safety agencies have largely transitioned to cradlepoint connections inside their emergency vehicles to allow full connectivity with a single device. This makes accessing CAD information, real-time video from UAVs or other personnel, or incident command information to report or receive critical data almost an intuitive activity.

The devices in the hands of law enforcement, firefighters, and other first responders are individually authenticated via a biometric handshake between the user and their device. Emerging screen flexibility technologies allow these devices to be rolled up so that they are small enough to fit in a pants pocket and then expanded to be large enough for use in tabletop emergency planning. An officer's visual broadcast capabili-

[3] Einstein originally said this during a 1929 interview with the *Saturday Evening Post*. The *Post* republished the quote in a 2010 article (Nilsson, 2010).

ties (now the size of a shirt button or name tag) allow others to dial in as they wish and can be called up by peers and supervisors to check the officer's status. The footage from the officer's broadcast information is seamlessly transformed into a police or fire report. This report is then forwarded to supervisors for review, to medical facilities so they can prepare for incoming patients, to custody facilities so they can triage mental health issues and placement priorities, and to prosecutor's offices to prepare warrants or charging papers.

The hyper-increased demand for broadband access because of video footage and the explosion in IoT devices in homes, cars, and businesses has created a need to continue work to share bandwidth with more and more "network slicing" of available bands. Broadband for law enforcement and public safety as part of the NPSBN is complete. Although AT&T was awarded a renewal of its contract in 2027, several potential future broadband partners are already vying for the next generation's build-out of the NPSBN.

The road from 2022 to our envisioned future has not been without challenges. The fragmented nature of law enforcement—with 18,000 agencies making sometimes independent, occasionally underinformed, decisions about broadband providers—and the dizzying array of enhancements in broadband technologies led some agencies not to act and others to spend money more than once to acquire the systems and capabilities they wanted. Others, though, led the way to collaborate, consolidate, and regionalize communications networks that formed the backbone of what is available today. After the stresses of the early 2020s, police, fire, and EMS agencies developed a consolidated network of interoperable platforms that actually work—one in which any cop can talk to any firefighter, and they can talk and send data to any incident commander, without giving a second thought to the technologies that they are using. Then again, there is always something out there that could be done to make first responders' communications better, so leading-edge chiefs and sheriffs are already thinking about what might come next. They know what their contemporaries in 2022 knew—that it was not as important to know the future as it is to make good decisions today to enable it to emerge.

APPENDIX A

Current and Emerging Broadband Technologies

Generations of Broadband

Understanding broadband technologies and how they developed might be as confusing as the myriad of wires, screens, radios, and keyboards in the modern police patrol car that supports the critical work of the contemporary police officer. Unlike other drivers on the road, the police are not driving for pleasure or to move from point A to point B. They use their cars to respond to routine and emergency calls, to be visible to others to deter crime, and to be where the public needs them during times of crisis. The key component of the dizzying array of technology in a police car is guaranteed, timely communication for the public's safety. This is critical for both routine operations and emergency incidents, during which officers communicate with their dispatch centers, officers and deputies communicate with one another, and, increasingly, the police are in direct contact with members of their communities.

To make the best-informed decisions about public safety broadband needs for the future, decisionmakers should explore two parallel issues: (1) the eras of broadband and the capabilities they enabled and (2) the standards and issues related to the deployment of mobile broadband for voice-data integration, PTT capabilities, and the intensifying need for added technology capacity to deal with UAS and similar emerging communications needs.

1G

There really was no "1G" when Bell Labs's Advanced Mobile Phone System (AMPS) was used in Chicago. This generation of broadband was retroactively named as the following generation of networks emerged. AMPS is an analog system; it took 12 years for the FCC to approve 40 MHz of spectrum in the 800-MHz band to use in 1983 (Ghosh et al., 2011). The use of analog radio waves meant limited mobile voice capabilities and data transmission speeds of up to 2.4 kbps. The first generation of mobile communications ended about ten years later as hardware platforms improved processing capabilities over time, paving the way for the second generation of broadband.

2G

Although carriers across the world switched to 4G LTE standards in 2010, U.S. telecommunications providers continued to support their legacy 2G systems through 2020 (Segan, 2020). That has changed, however;

Verizon turned off its CDMA network at the end of 2020, Sprint sunset its 2G CDMA network in December 2021, and T-Mobile is planning to turn off its 2G network in December 2022.[1]

3G

As standards were consolidated and end-user speeds increased, IMT-2000 evolved to accommodate data transfer speeds of up to 2 megabytes per second (MBps) (Ghosh et al., 2011). Although 3G technologies afforded users much faster data speeds and more-reliable voice communications, the inability of CDMA and GSM technology platforms to support mobile devices (as evidenced by Verizon's intent to abandon CDMA and Sprint's intent to discontinue GSM) presented issues in a world that was increasingly becoming interconnected. 3G saw advances in both voice and data transmission speeds, most notably Evolution–Data Only (EV-DO), developed by Qualcomm to achieve higher data rates (Ghosh et al., 2011). CDMA/EV-DO, introduced in October 2000 to improve data transfer speeds, was upgraded by 2002 to full broadband-like speeds and had more than 120 million subscribers by 2009 (Ghosh et al., 2011). Mobile 3G accelerated transfer speeds up to 63 MBps; however, as High-Speed Packet Access (HSPA) improves downlink speeds, it sets the stage for even faster speeds to meet existing and emerging data transfer demands.

In the 3G era, users saw enhanced video and audio speeds, higher data transfer speeds, support for videoconferencing, and much higher web browsing speeds. 3G also enabled technologies to stream television over the internet. In 2001, IEEE developed standards for a wireless metropolitan-area network, which led to the development of the Worldwide Interoperability for Microwave Access (WiMAX) in 2007; WiMAX elevated peak data rates to as high as 74 MBps (Ghosh et al., 2011).

4G

Cable (wired coaxial lines run to the user's device, usually a home computer) and digital subscriber lines (DSLs), which transmit digital data via regular phone lines, are the dominant means of broadband connection in the United States, although the use of fiber-optic networks is growing and accounted for almost 14 percent of broadband connections by 2018 (Hightower, 2019). DSL is the most prevalent means of data transmission in the world and is especially critical in rural areas, where phone connection is ubiquitous. By 2016, 89 percent of U.S. households had computers, and 81 percent had broadband internet subscriptions (Ryan, 2018). Of particular interest to the mobile broadband community, 76 percent of these households had smartphones by that time (Ryan, 2018). Cable and DSL provide users with fast, reliable connection to the internet, and a growing fiber-optics sector means that data transmission speeds may experience significant and sustained increases over time. As smartphone usage becomes more widespread, and as subscribers demand speeds they experience at home or work, the need for interoperability among differing networks and platforms continues to intensify.

To meet growing demand for high-bandwidth applications, continued exponential growth of smart mobile devices, and sustained competition among broadband providers, LTE was intended to

- deliver performance at levels roughly equivalent with wired broadband, which means that transfer speeds would be an order of magnitude faster than 3G download and upload speeds

[1] The specific dates on which various 2G and 3G systems will be turned off vary from country to country, and the announced dates of decommissioning any particular network may be extended at the provider's discretion. Dates listed here are from Remmert, 2021.

- coexist and work with existing 3G and non-3GPP systems to enable service continuity as a mobile user roams across networks
- reduce the cost per megabyte to deliver data to end users, a key element in the design criteria for LTE (Ghosh et al., 2011).

Although many people with smartphones or similar devices might believe their devices are 4G, they can also see the abbreviation "LTE" following the 4G reference. LTE is an evolution of the Universal Mobile Telecommunications System (UMTS)/3GPP 3G standards that uses a different form of radio interface (it is no longer a platform for 3G CDMA access to radio networks) but does not reach the speed or response times set by the ITU in cooperation with 3GPP for 4G devices. For instance, the ITU set a speed and connection standard of a peak of 100 MBps in 2008 (Hill, Chandler, and Beaton, 2021). 4G also does not use circuit switching. Instead, it operates on an all-IP-based communication platform, including Voice over Internet Protocol (Koh, 2020).

In response to what was seen as possibly unreachable minimum speeds to qualify as 4G, the ITU decided that technologies used in pursuit of 4G standards would be termed LTE. Networks soon began advertising their connections as "4G LTE" even though those networks did not meet the requirements to be termed as such (Hill, Chandler, and Beaton, 2021). Another area of confusion is the use of the term LTE-A. LTE-A does achieve the standards set by the ITU. It uses Carrier Aggregation to achieve increased data rates per user, and it employs better multi-antenna techniques to increase speed and stability (Koh, 2020).

WiMAX

A final term to consider with regard to 4G LTE is WiMAX, another type of wireless broadband. Although it was initially seen as a candidate for 4G networks, its use is decreasing. However, it is still in general use and is used for "last mile" links (Electronics Notes, undated). The first generation of WiMAX was faster than LTE, but still below 4G standards. WiMAX Release 2, however, is a true 4G connection, with comparable download and upload speeds to those of other types of 4G. WiMAX, like Wi-Fi, allows users to create wireless network connections. WiMAX can cover distances similar to those of other cell networks, which means that users can employ a desktop or a laptop from almost any location (Spector, 2010).

Voice-Data Integration

Although voice/data phones have been marketed since 1993 (Reed, 2010), Apple's unveiling of the iPhone in 2007 integrated data and voice functions through a touchscreen display, web browsing, time and geolocation services via GPS, cameras, and motion sensors, and the iPhone remains the standard against which all other portable communications devices are compared (Reed, 2010). Today, any one of the more than 2 billion smartphones in use worldwide has more computing power than the entire National Aeronautics and Space Administration had when it put the first astronauts on the moon in 1969 (Level Education, 2016). First responders, though, have lagged in the development of systems, networks, and platforms to support the integration of the smartphone and related mobile broadband technologies into the array of communications capabilities they possess.

Although commercial carrier broadband networks are nearly universal in the United States, with a handful of exceptions, they do not support the quality of service required for mission-critical communications in many instances. This issue led to the creation of P25 in 1990, in response to the FCC's 1987 action that set aside 6 MHz of spectrum in the 800-MHz band for exclusive use by local, regional, and state public safety agencies under guidelines developed by the National Public Safety Advisory Committee (FCC, 2018). In response to the FCC's announced intent to mandate trunking standards, APCO International led work by several national associations and government agencies to create standards for interoperable emergency communications (ICOM, 2008).

Project 25 Standards

In 1990, Project 25 (P25) was established in the United States in the aftermath of FCC mandates to improve very high frequency and ultra high frequency use for public safety and to open the 800-MHz band to

- develop a digital radio standard for public safety
- create an ease of use and interoperability among public safety agencies
- use radio frequencies in a spectrally efficient manner by multiple vendors in a frequency-independent environment (Project 25 Technology Interest Group, 2016).

P25 enabled the use of digital transmission technologies for voice and data with global standards and created pathways to migrate away from legacy equipment. It was intended to be a user-driven LMR standard. In addition to P25's goal of enhancing voice transmissions, P25 standards served the goal to create a platform from which data could be exchanged between headquarters and personnel in the field using MDTs.

Project 25 Phase II

Beginning in 2011, P25 transitioned to a "Phase II" to optimize the use of narrowband communications (P25, undated). Narrowbanding uses a much smaller portion of an allocated frequency bandwidth for voice communications, thus facilitating radio availability for more agencies and enabling data transfer to radios (Griffith and Clark, 2014). Phase II began even as the more advanced LTE standard in commercial mobile phone networks encouraged the development of hybrid radio devices for first responders that have both smartphone capabilities (LTE) and P25-compliant LMR functions (Griffith and Clark, 2014). However, the September 11, 2001, terrorist attacks tragically identified many of the communications deficits of interoperability and adequate bandwidth for mobile communications that first responders must contend with during mass casualty events and disasters. Although it took more than a decade, Congress created the NPSBN as part of the Middle Class Tax Relief and Job Creation Act of 2012 (Pub. L. 112-96, 2012).

PTT, POC, OTTPTT, and MCPTT

Since the inception of the two-way radio and subsequent LMR systems, the police have used a PTT process on their radios. The 800-MHz band, though, offered an opportunity to develop devices (e.g., the cell phone) that could make direct-dial voice calls and also offer a PTT-over-cellular (POC) function. In 1993, Nextel, using Motorola's Integrated Digital Enhanced Network (iDEN), launched a nationwide PTT phone that kickstarted the development of similar platforms and devices by its competitors. After Nextel's 2005 merger with Sprint, the original POC was made interoperable using QChat technology in 2008. By 2013, Sprint ceased service on its iDEN network, transitioning POC subscribers to its 3G Pattern Division Multiple Access (PDMA) "Direct Connect" platform. Verizon and AT&T entered the POC market at the same time, providing 3G carrier-integrated POC (Seybold, 2017a). In addition to the carrier-integrated POC, new suppliers had begun offering OTTPTT. By 2017, the major wireless carriers offered carrier-integrated POC, and others offered OTTPTT on and across multiple networks; the dominant supplier was Enterprise Secure Chat (ESChat), which served military, public safety, utility, and transportation companies (Seybold, 2017a).

Public safety LMR systems have long provided, and will continue to provide, mission-critical communications for law enforcement. To serve the growing needs of public safety, however, agencies have shifted non–mission-critical communications to commercial cell providers. With the emergence of the NPSBN and its vision of providing new features and capabilities, FirstNet has deployed an MCPTT functionality (AT&T, 2018), which allows police and other first responders to use a single mobile device for voice and data purposes that is interoperable across LMR/LTE platforms (National Public Safety Telecommunications Council, 2018). To do so, FirstNet and other providers will have to continue to address deficits in commercial PTT systems. This includes achieving parity with legacy systems, creating native integration in devices, and providing preferential access to radio resources (GSMA, 2017).

5G

To sum up the current state and probable future of broadband communications, 1G is analog cellular. 2G technologies, such as CDMA, GSM, and Time Division Multiple Access (TDMA), were the first generation of digital cellular technologies. 2G was largely responsible for facilitating the expansion of cell phones to the general public. 3G technologies, such as EVDO (Evolution—Data Optimized or Evolution—Data Only), HSPA, and UMTS, raised speeds from 200 Kbps to a few megabits per second. That generation, which is still in wide use throughout the world, enabled smartphone apps to be used ubiquitously and created a foundation for the modern communications device as most know it. 4G (WiMAX and LTE) scaled up to hundreds of megabits and even GB-level speeds. 4G and 4G LTE reached the market at about the same time, leading to confusion and a misunderstanding of 4G LTE as a true 4G technology (McCallion, 2022). FirstNet, Verizon, and others that market public safety prioritization, preemption, and PTT are all largely placing these capabilities on 4G LTE platforms. 5G brings three new things to the table: bigger channels to speed up data, lower latency to be more responsive, and the ability to connect many more devices at once (for sensors and smart devices).

5G operates across a fairly broad bandwidth. Low-band 5G operates in frequencies below 2 GHz, the oldest cellular and television frequencies, covering great distances, but with few wide channels to handle the volume of use. Low-band 5G is slow and has similar speed characteristics as 4G. Mid band is the 2–10-GHz range, which includes most current cellular and Wi-Fi frequencies. Mid band has a decent range, and these frequencies are the workhorse frequencies for 5G in most countries other than the United States. High-band 5G, or *millimeter wave* (mmWave), is in the 20–100-GHz range. High-band 5G is new for consumer applications; it has a shorter range (about a maximum distance of 1,500 ft from towers for mmWave 5G) but vast amounts of unused spectrum, which means very fast speeds using up to 800 MHz at a time. With regard to 5G range, it is important to note that Qualcomm and its partners have completed the world's first extended-range 5G New Radio (5G NR) data call over mmWave, achieving a 3.8-km distance (Qualcomm, undated).

5G's speed potential adds the opportunity for greater data security, since the speeds allow for more data encryption. 5G networks all still need 4G networks and coverage to establish their initial connections (e.g., they are not yet stand-alone). There is still no standard for 5G for voice (Segan, 2022). One drawback to 5G on its higher (and faster) bands is that the wavelength is very short, meaning that data can be transferred more quickly, although the transfer distance is shorter than that of a 4G device.

No matter which generation of technology (or combination of technologies) is deployed by law enforcement for public safety broadband, there are applications that have already come online that will affect not only the demand for broadband but also its effectiveness in real time to transmit voice, data, and video. Two applications of note are the use of UAVs and the use of COLTs and COWs.

Unmanned Aerial Systems Management

The rapid emergence and mainstream adoption of UAS for commercial, government, and public safety uses has pushed considerations of data transfer and communications issues related to UAS to the forefront. These uses are as diverse as food and package delivery, infrastructure inspection, flights of emergency medical equipment, proof-of-concept testing of future air-taxi technologies, and ways to sustain communications and control of UAS flying beyond the lines of sight of their operators (Shepardson and Dastin, 2018). The City of Chula Vista, California, is working with the Federal Aviation Administration and the City of San Diego to support innovation related to public safety UAS deployment (Van Grove, 2018) and is in the midst of a pilot Drone as First Responder (DFR) program in 2020.

The use of drones varies, from ad hoc deployment by scene managers at critical incidents to DFR deployment to strategically support officers in the field for a variety of critical and routine activities. For all uses, however, real-time video, low latency in transmissions, and the ability of ground personnel to maintain consistent control of the UAS at all times are minimum thresholds for the continued integration of UAS into service for police, fire, and EMS agencies. Those objectives are consistent with the LMR/LTE needs of law enforcement for all other communications needs and will be increasingly important aspects of the needs of police with regard to public safety broadband.

COLTs and COWs

Cell and other communications towers have the disadvantage of requiring a great deal of fixed infrastructure to lift antennas high off the ground; thus, they have the largest possible line-of-sight coverage area. They are also subject to going offline during major incidents because of power loss or direct damage to their electronics or structure. COLTS and COWs provide broadband over large rural areas without broadband infrastructure, as well as areas in which infrastructure has been taken offline. Participants in NIJ's Broadband Communications Workshop called for considering the use of flying vehicles as airborne broadband communications relays. The panelists considered this issue important enough that it was ranked third of almost 70 total needs to help law enforcement employ broadband communications (Hollywood et al., 2016, p. 1).

Such systems are starting to be fielded. For example, the NPSBN (FirstNet) is now offering tethered UAVs as part of its emergency response fleet. These are "flying COWs" that relay Band 14 communications. Their flying height is 400 ft; in contrast, cell towers are typically below 350 ft. As of 2019, FirstNet has three flying COWs in its inventory (Bostic, 2019). It also has a tethered aerostat, "FirstNet One," which can fly as high as 1,500 ft and is designed to cover an area five to six times that of a COLT (Jackson, 2020).

COWs, COLTs, Cell Sites on Wheels (CSOWs), and SatCOLTs are mobile cell site units of varying sizes and capabilities. In essence, they are mobile cell towers designed to support cell usage (data and voice) in emergencies, disaster zones, and planned large-scale events during which normal cell service is either disrupted or saturated because of the sheer number of users or data load present. Although these tethered airborne relays are intended for short-term incident response, over the next few years, they might become options for persistent coverage in rural areas in lieu of fixed ground-based approaches.

COLTs, COWs, and their variants provide a temporary data infrastructure and can restore an existing network whose fixed cell towers have been destroyed or taken offline through a loss of power or similar means. Depending on the specific need and the length of time they would be used, COWs and COLTs can provide first responders reliable and uninterrupted service as needed to cope with hurricanes, earthquakes, and sustained emergency operations. They can also be deployed for preplanned events, such as a NASCAR event, college and professional football games, or Olympic-level sports festivals.

COWs, COLTs, SatCOLTs, and CSOWs are terms used loosely and interchangeably to describe any portable mobile cellular sites that provide temporary network and wireless coverage to locations where cellular coverage is minimal or compromised (Techopedia, undated). They can be used for short- or long-term deployment to areas with nonfunctional stationary cell towers. Generally, COLT denotes a smaller, more portable, and less robust system. COWs are traditionally trailers that are hooked to a tractor-trailer rig to be towed to a location (Basich, 2009).

There is very little information on the development or history of mobile cell sites, although 36 COWs were deployed following the 9/11 attacks and multiple COWs were used for emergency communications after Hurricane Katrina (Kramer, 2017). The use of blimps, UAVs, and other aerial support systems is a glimpse of the future. COWs, COLTs, and their support systems will continue to be deployed and used on a recurring basis for emergencies and planned events, and some COWs can be semipermanent for underserved populations as an interim measure while these populations wait for permanent cell towers to be built.

Public safety agencies and their LMR-LTE providers might want to assess the cell capacities of their systems in normal and emergency operations and plan for ways that COW and COLT deployment can support communications during natural disasters or large-scale planned events. These plans should be part of an agency's emergency operations plans, and staff should be trained in how to make appropriate requests from their providers.

5G, 5G E, 5G+, and Other Emerging Advances

In 2022, there is a considerable amount of confusion concerning 4G, 4G LTE, 5G, and 5G Evolution (5G E). Each broadband provider has its lexicon of what a particular generation is termed, and each employs a different technological methodology to serve its customers. This is a matter of the technological platform, repeaters, and reception in any particular area, as well as the call and data load of denser urban areas. In truth, as 5G begins to be available to law enforcement and the consumer market, it will rely on 4G transmission technologies for parts of its data load until sufficient 5G infrastructure exists.

Some users might see a "5G E" platform on their AT&T phones, which is similar to what happened when carriers were able to deliver some, but not all, 4G speeds and began to describe their services as 4G LTE. 5G E has some, but not all, of the technological standards to be a true 5G platform. For instance, the symbiosis of 4G and 5G led AT&T to call its 4G network 5G E. End-user confusion is likely to continue for the foreseeable future, not only as providers seek to gain a competitive advantage as their technologies improve but also because there are three bands within which 5G can be used and several approaches to combine 5G with 4G to enhance upload and download speeds and the delivery of voice and data.

The industry (3GPP) has settled on 5G NR as the standard to fulfill 5G specifications for the U.S. market. 5G NR can use wider channels, communicate better with remote servers (lower latency), and load more data into a radio cycle than 4G (Segan, 2019). 5G opens up high-band (mmWave) spectrum—very fast short-range airwaves that do not work with 4G. 5G can run on any frequency, however, so there are three different 5G experiences—low-, mid-, and high-band transmissions. This allows carriers to flexibly share between 4G and 5G, to "stack" channels for greater speeds, and to split channels between 4G and 5G based on demand. In July 2020, AT&T announced 5G+ service, which runs in the mmWave spectrum and is available in 35 cities. A *Wired* article describes low band as below 1 GHz, mid band as 1–6 GHz, and mmWave as above either 24 or 30 GHz (Finley and Pearlstein, 2020). The authors also note unlicensed spectrum, which is available to all carriers for ranges now used for home Wi-Fi. They say that the mid band is the "sweet spot," since it has broad geographic reach and is faster than low band. To enable 10-gigabyte-per-second (GBps) speeds, however, networks must use mmWave (mid band is 1 GBps) (Finley and Pearlstein, 2020).

To take advantage of 5G, users must have 5G devices. Most major vendors have 5G devices available to the general public; both AT&T/FirstNet and Verizon have 5G devices listed for sale for their public safety clientele. Huawei is the world leader in 5G network equipment but is not, and might not be, used in the future for U.S. applications (Finley and Pearlstein, 2020). Verizon relies on high band, which it calls "Ultra Wideband." AT&T describes it as "high band" or "5G+." AT&T has 5G+ in 35 cities, and T-Mobile has 5G in in seven cities. In 2022, Verizon serves 100 million people with its C-band 5G, and it expects to provide Ultra Wideband 5G to 175 million people by the end of 2022 (Alleven, 2022). To use high band, cellular providers will have to use many smaller, low-power base stations or more-powerful macrocells to offer mmWave speeds. 5G uses orthogonal frequency-division multiplexing (OFDM) coding, which is similar to 4G LTE coding. This interface is designed for much lower latency and greater flexibility than LTE. With the same airwaves as 4G, 5G gets about 30 percent better speeds because of more-efficient coding.

Into the Future—5G and Beyond

For the next few years, 4G LTE should suffice for law enforcement connectivity and mission-critical communications services. As providers transition their platforms to faster and more-robust 5G networks, though, public safety users will inevitably want the speeds necessary to facilitate real-time data streaming (from body cameras, UAVs, and other devices), to expedite data uploads and downloads for incident management and data analysis, and to ensure large-scale interoperability without concerns about latency slowing the speed of voice. Residential and commercial users will be able to better connect and use such devices as home thermostats and environmental sensors. Some of the other advances that 5G will enable are

- communication within vehicles as they become more automated and move to autonomous driving
- communication of vehicles with smart roadways to manage traffic and roadway safety
- virtual and augmented reality functions, which will operate at speeds (and without latency) that enable such functions as holographic remote surgery and other uses that require real-time responsiveness
- "mixed reality" that combines augmented reality and virtual reality for both entertainment and industry purposes, with interactive data that could allow lightweight headsets to overlay maps, business functions, and productivity apps with actual and virtual realities
- the speed and capacity for any devices or technologies seeking to create an IoT ecosystem to deploy robots, have devices interact, and enhance safety measures for workers
- smart cities, which will become the norm, with 5G speeds tracking traffic conditions, parking availability, refuse pickup, and guidance to smart vehicles to avoid congestion (Newman, 2019).

Each of these advances will directly or indirectly affect law enforcement and public safety. They could also create a path to select an LMR/LTE combination for communications, or they could lead to a migration away from LMR to a 5G-enabled voice and data platform of the future.

These transitions are not going to happen overnight, but major shifts due to 5G should be expected in the next five years. Qualcomm predicts that there will be 200 million 5G subscribers by the end of 2020 and 2.8 billion 5G connections by 2025 ("When Is 5G Coming to You? The Definitive Guide to the 5G Network Rollout," 2021). In September 2020, AT&T announced that it was going to deliver 5G and "Networking-as-a-Service capabilities" to three U.S. Air Force installations to "optimize the value of our 5G and other networking capabilities" (AT&T, 2020), and, in October 2020, the U.S. Army selected FirstNet for its U.S. installations ("U.S. Army Selects FirstNet, Built with AT&T, for Public Safety Communications Across 72 Installations in the U.S.," 2020). Law enforcement users should be aware that a true 5G platform will require 5G devices, although 5G, like its predecessors, should be backward compatible with 4G devices and systems.

Law enforcement agencies across the United States will expand their use of broadband networks through FirstNet or similar means for the foreseeable future. The commitment by AT&T (and its commercial competitors) to create and sustain the core network and link it to AT&T's commercial infrastructure will provide an opportunity to take advantage of the bandwidth necessary to transmit photo, video, and data files. At the same time, the physical infrastructure needed to ensure that the system's prioritization remains intact is still in question. In spite of that, some agencies have moved to implement law enforcement broadband communications and are "first movers" from which others can learn.

LA-RICS is one of the country's first movers in acquiring, managing, and using LTE networks for law enforcement and other first responders. LA-RICS constructed "75 public safety grade broadband sites," including 13 COWs, as a part of a Broadband Technology Opportunities Program grant awarded in 2010 by the National Telecommunications and Information Administration (Wendelken, 2017). Shortly after California opted into FirstNet, LA-RICS and AT&T finalized an agreement to transfer and assign the LA-RICS public safety broadband network to AT&T (Wendelken, 2017). Because the AT&T network will rely on AT&T's existing and emerging commercial infrastructure (instead of mission-critical, public safety–grade broadband sites, which are only loosely defined), it is unknown whether the planned system would remain functional in the case of a significant seismic event, another large-scale natural disaster, or a catastrophic incident like 9/11. One issue for the NPSBN and any other first responder mobile broadband service is that no matter how law enforcement and other first responders might be prioritized, the system must be intact for the prioritization to be relevant to the management of their response.

The emergence of 5G technologies will add to the complexity of the issue and warrants research and evaluation to identify agencies that are leading in the deployment of broadband technologies and study their deployments. The ideal research effort would result in a scalable set of best-practice methodologies that document conceptual and existing network architectures and field deployments in a variety of demographic and topographic settings. Drawing on the experiences of LA-RICS and others, researchers should evaluate a mix of local, regional, and blended approaches to the integration of broadband technologies to create a national guidance document. This document (or series of documents and scholarly articles) should address the myriad of law enforcement use cases and approaches used to filter, prioritize, and analyze data sent over the network.

The document, and its findings and considerations, should also assist in the research and evaluative processes, policies, and human factors regarding the migration from legacy systems and approaches to an integrated LMR/LTE network (or 5G/LMR integrated network) as it is currently being developed by FirstNet and others. The long-term benefit of such work will be to help determine a best path forward as 5G and other systems become available in the next decade. If done well, law enforcement communications will be interoperable as envisioned, with uninterrupted first responder coverage as described by the FirstNet Authority Board and FirstNet/AT&T.

APPENDIX B

Full Results of Coverage Modeling

In this appendix, we present the full information and results for the coverage modeling briefly mentioned in Chapter Seven.

To demonstrate the suitability of the different technologies for police use, we conducted coverage modeling using the Naval Research Laboratory Builder radio frequency modeling package. This allows the reader to visually assess the similarities and differences among the LTE frequency bands, FirstNet's band, and the 5G and LMR bands. Each map (Figures B.1–B.9) shows frequency range and usefulness for mobile devices (and mobile LMR for that map) in a series of colors. The area where there is no color indicates no frequency coverage; red indicates a poor connection with low reliability; yellow represents coverage that is better, yet still poor; and green indicates a reliable signal strength, one that an end user would see as a "3- to 5-bar" connection on their device. The figures in this appendix depict repeater coverage at four cell frequencies (778 MHz, 850 MHz, 1,900 MHz, and 4 GHz), coverage for both commercial and FirstNet mobile devices, and an LMR frequency coverage map. In this set of maps, the reader will see the following:

- Among the four LTE frequencies (778 MHz, 850 MHz, 1,900 MHz, and 4 GHz), the coverage is similar and does not significantly improve from one frequency to another.
- As frequencies rise from 778 MHz to 4 GHz, the effective coverage range decreases. 5G coverage is significantly reduced compared with the lower-frequency bands and would necessitate more repeater sites to create reliable coverage for public safety purposes. In addition, lower-frequency bands have better penetration through walls and obstacles and could therefore increase coverage inside buildings.
- A consumer cellular handset and a FirstNet handset were both assessed at 778 MHz. The FirstNet handset was shown to have a significant advantage in signal quality; however, if the "usable" range is considered equally good enough to achieve the mission, the two handsets are roughly comparable.
- The 100-W LMR/P25 repeater provides comprehensively better coverage, especially in terrain that is hilly and contains either natural or human-made obstructions. Because LMR is a reliable one-to-many communications platform, its coverage is well suited to continue to perform in that way for the foreseeable future.

The outcomes of the coverage modeling strongly suggest that the idea that LTE/5G will displace LMR in the near future is not supported by the evidence. Although broadband offers advantages in one-to-one communications and the transmission of voice and data over shorter distances, the reliable connectivity of communications among devices and base stations will be best achieved through a platform that uses the advantages of both LMR and LTE/5G in a seamless and integrated fashion.

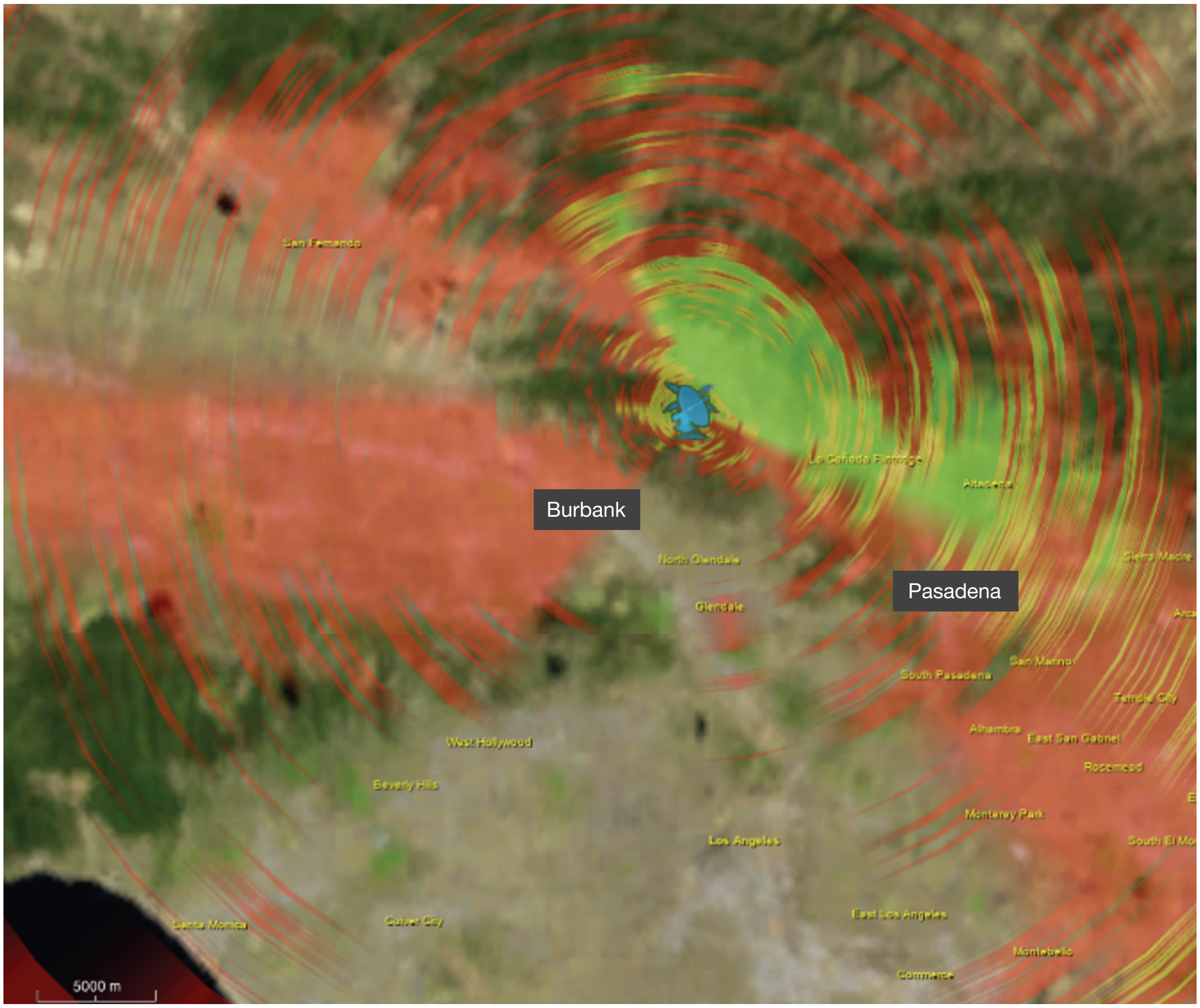
Our modeling was conducted using 30-m resolution Shuttle Radar Topography Mission, version 2, terrain data using the Terrain Integrated Rough Earth Model propagation model; in all cases, we modeled the transmitter as an isotropic antenna with vertical polarization. Unless otherwise stated, we used a max gain of 10 dBi[1] and a peak power output of 7.5 W, with the antenna broadcasting from 125 ft above ground level (AGL) at 34.2195412° north, 118.26863805° west, and the received signal strength being sampled at 6 ft AGL.

For our cellular cases, we used a scale where a received signal strength of less than –90 dBm[2] is considered unusable and displayed as red; greater than or equal to –90 dBm but less than –70 dBm is considered weak but potentially usable and shown as yellow; and greater than or equal to –70 dBm is considered a good connection and shown as green. Areas with none of these colors have no reception.

We chose the location to use for our modeling, displayed in Figure B.1, on the basis that there is a real tower there with both cellular and FirstNet transmitters. As can be seen in the figure, this location is on the side of a mountain, with another mountain only a few miles away on the other side of a valley. The signal from this tower also runs into the side of the mountain that it is sitting on as the signal goes to the northwest. This is reflected in all of our modeling results as showing good reception within the valley and bad recep-

FIGURE B.1

Cellular Tower, 778 MHz



[1] *dBi* refers to the forward gain of an antenna measured in decibels.

[2] *dBm* is an expression of power in decibels per milliwatt.

tion everywhere else. Towers placed on the side of the mountain closer to the ocean would have their signals extend significantly farther because of the lack of physical obstructions.

FIGURE B.2
Cellular Tower, 850 MHz

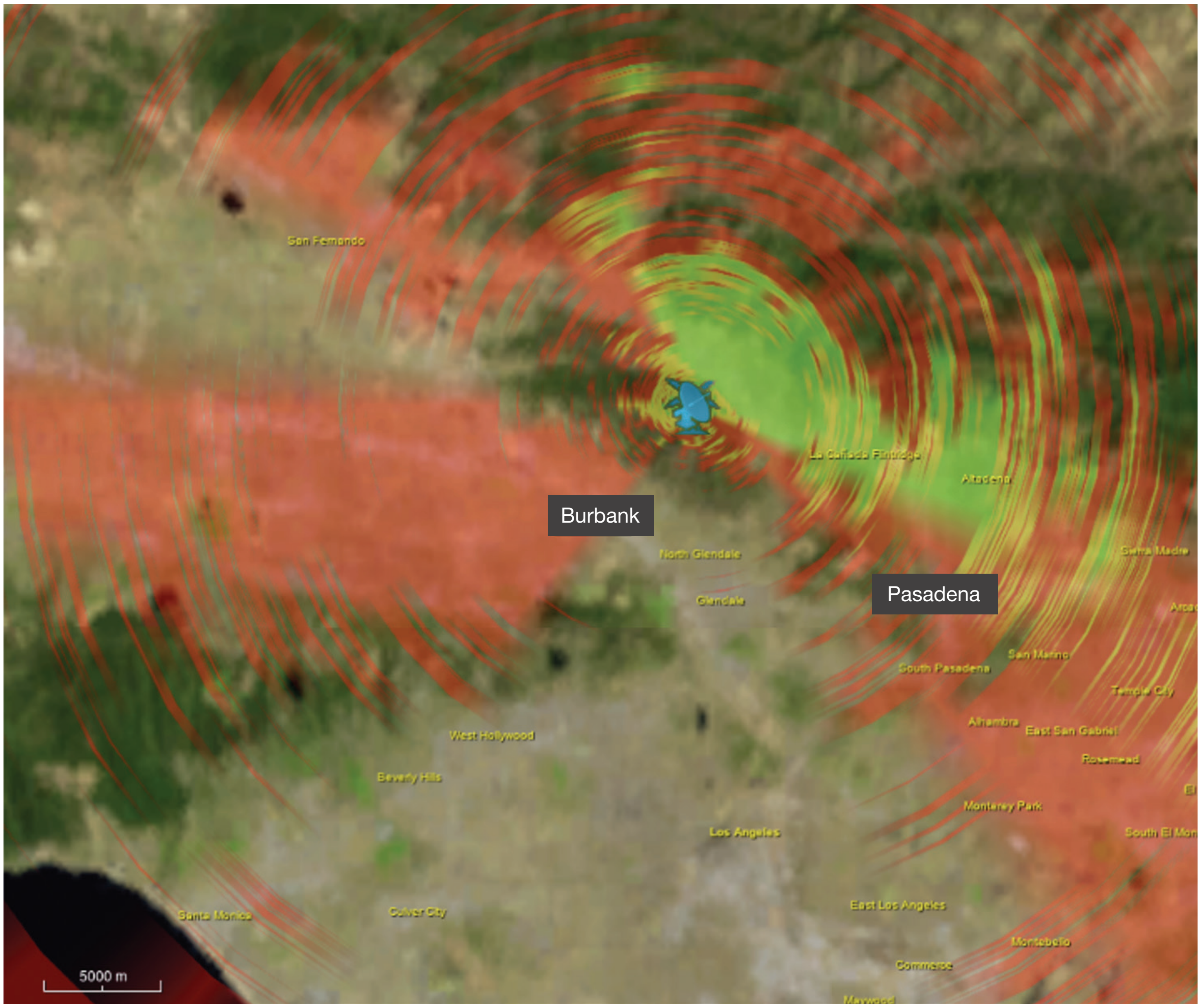


FIGURE B.3

Cellular Tower, 1,900 MHz

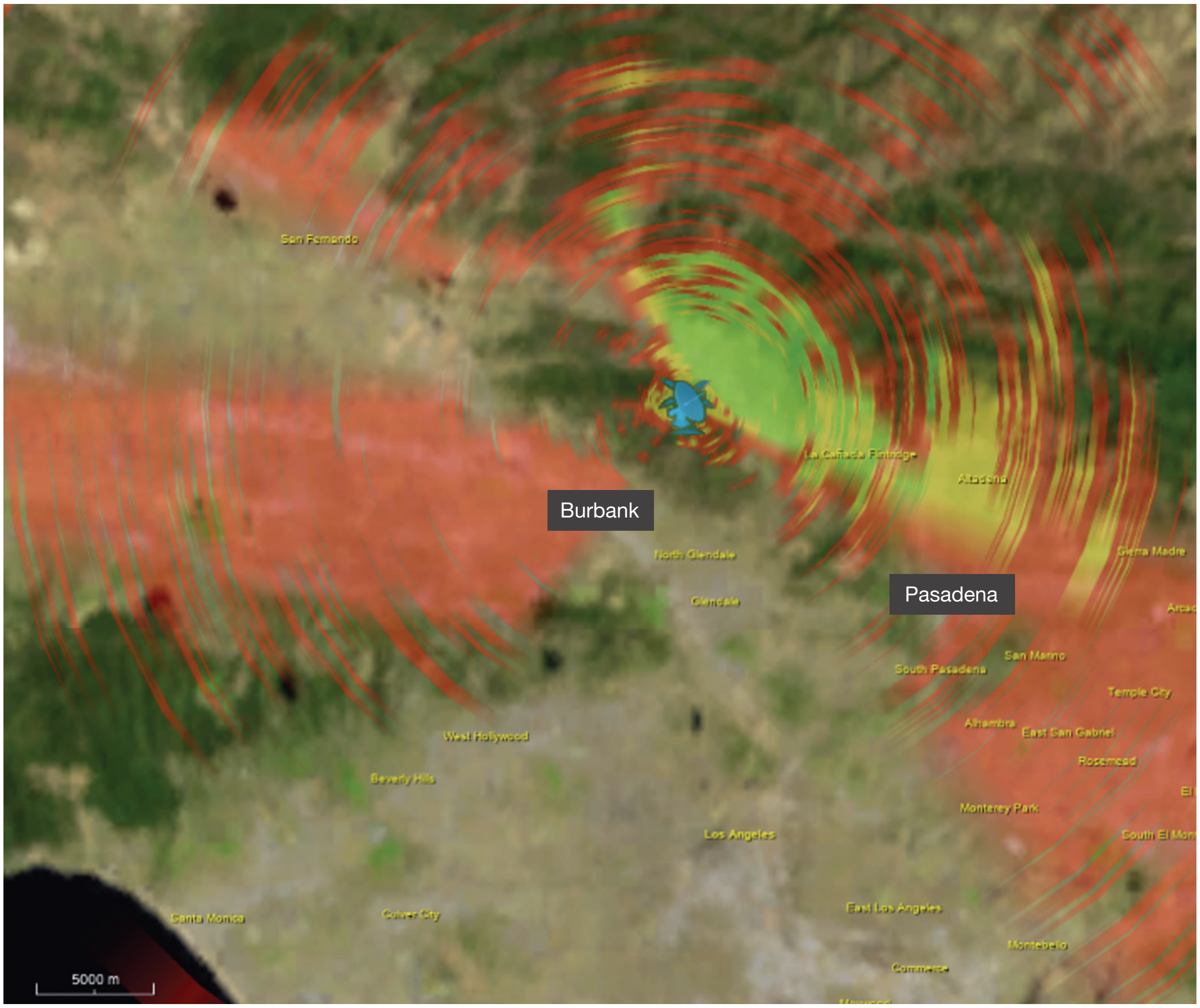
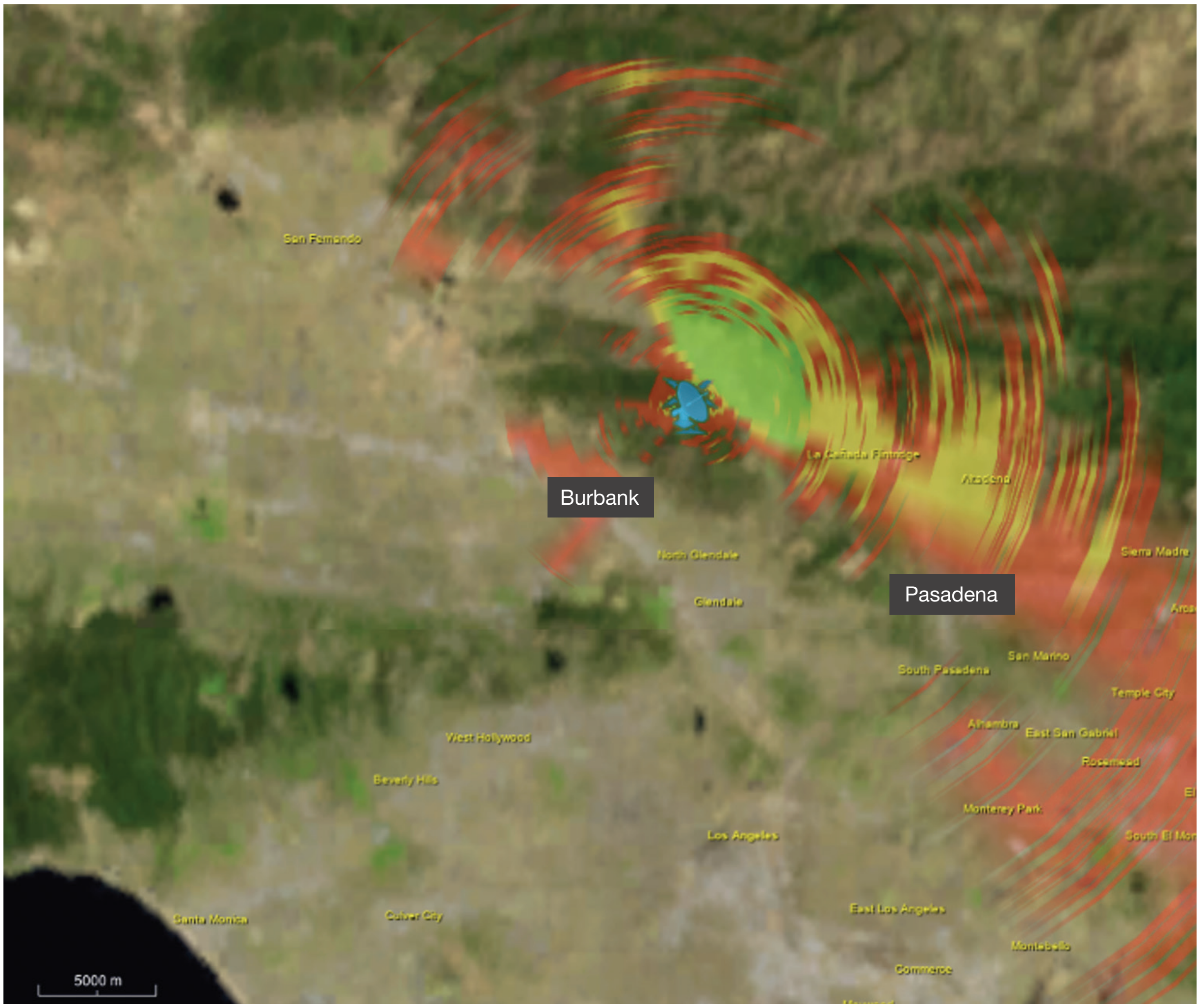


FIGURE B.4

Cellular Tower, 4 GHz



In our four cellular tower examples, we see that coverage is comparable from 778 MHz through 4 GHz. Most of the difference is in the areas with signal strength less than –90 dBm, which is not a usable signal.

Our two cellular handset cases are (1) consumer cell phones broadcasting at 778 MHz at 0.25 W and 2.2-dBi gain and (2) a FirstNet vehicular system broadcasting at 778 MHz at 1.25 W and 2.2-dBi gain.[3] We modeled these as being at the cellular tower location at the 125-ft AGL elevation used for the tower; our justification for this is that a handset broadcasting from the tower location to a point 6 ft off the ground is equivalent to a handset at 6 ft off the ground broadcasting to a tower 125 ft off the ground.

[3] The higher power drain associated with higher signal output makes it less than ideal for handset applications, and none are currently available on the market. However, there are vehicular cellular systems available on the market that could take advantage of the higher transmit power.

FIGURE B.5

Consumer Cellular Handset

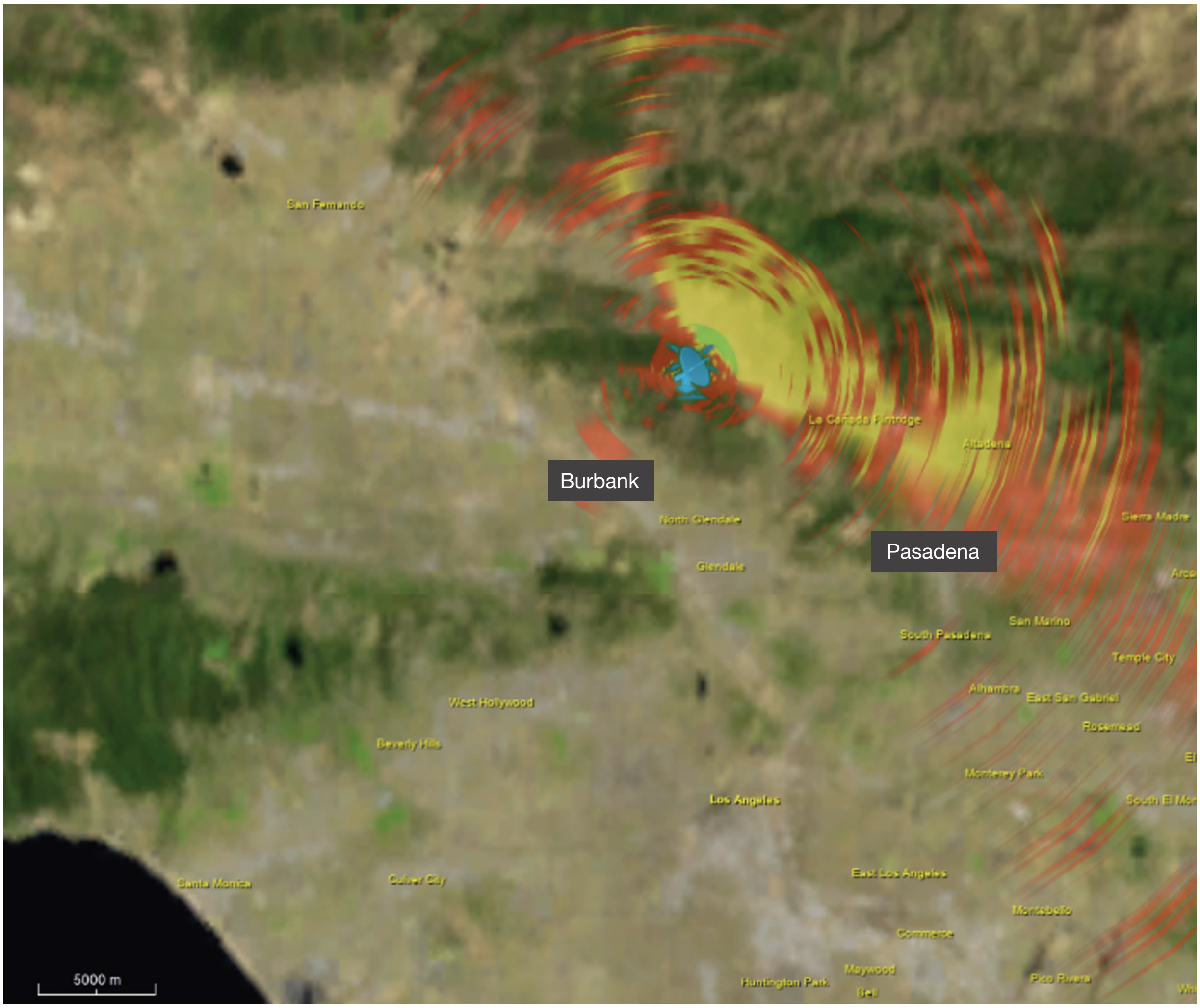
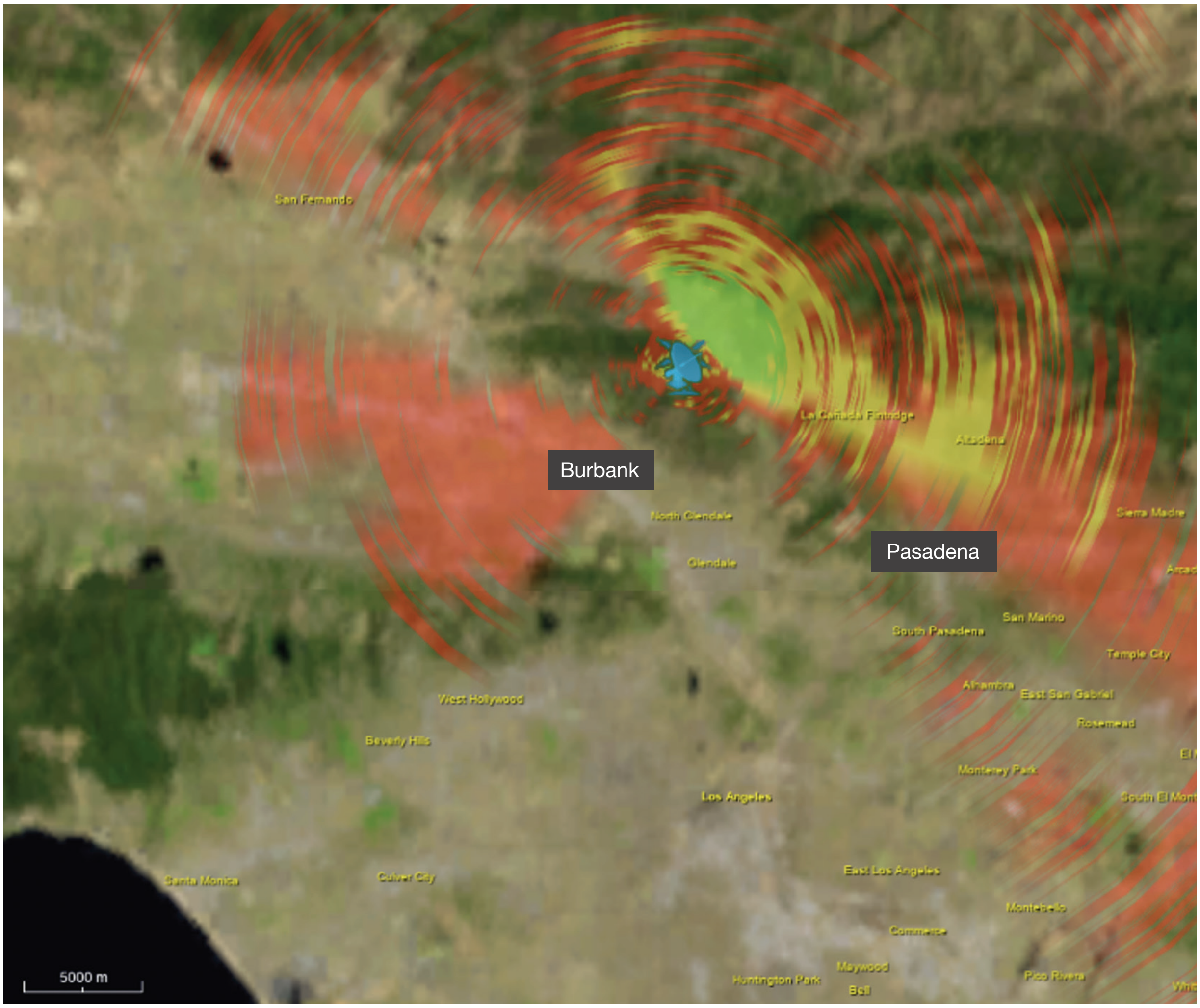


FIGURE B.6
FirstNet Cellular Handset



In this case, we see that the FirstNet handset has a significant advantage in signal quality coverage, but if the “usable” range is considered equally good enough to achieve the mission, then the two handsets are roughly comparable.

For our LMP/P25 examples, we considered any received signal strength of greater than –110 dBm (DAQ [data acquisition] 3.4 or better) to be a good signal and colored the area green. We considered a signal strength of less than –110 dBm but greater than –120 dBm (DAQ 3) to be barely usable and colored it red, and we considered anything less than –120 dBm to be unusable and did not shade it on the map. Our first case is an LMP/P25 tower broadcasting a 700-MHz signal at 1,000 W and 2.15-dBi max gain at the cellular tower elevation of 125 ft AGL. Our second case is a car antenna broadcasting at a 25-W peak power output at the 125-ft AGL elevation; we used the same justification that we used for having the cellular handsets broadcast from 125 ft. The third case has a car antenna broadcasting from the same location but from 6 ft AGL; this case models direct car-to-car LMP/P25 communications without routing the signal through a tower.

FIGURE B.7

1,000-W Land Mobile Radio/Project 25 Tower

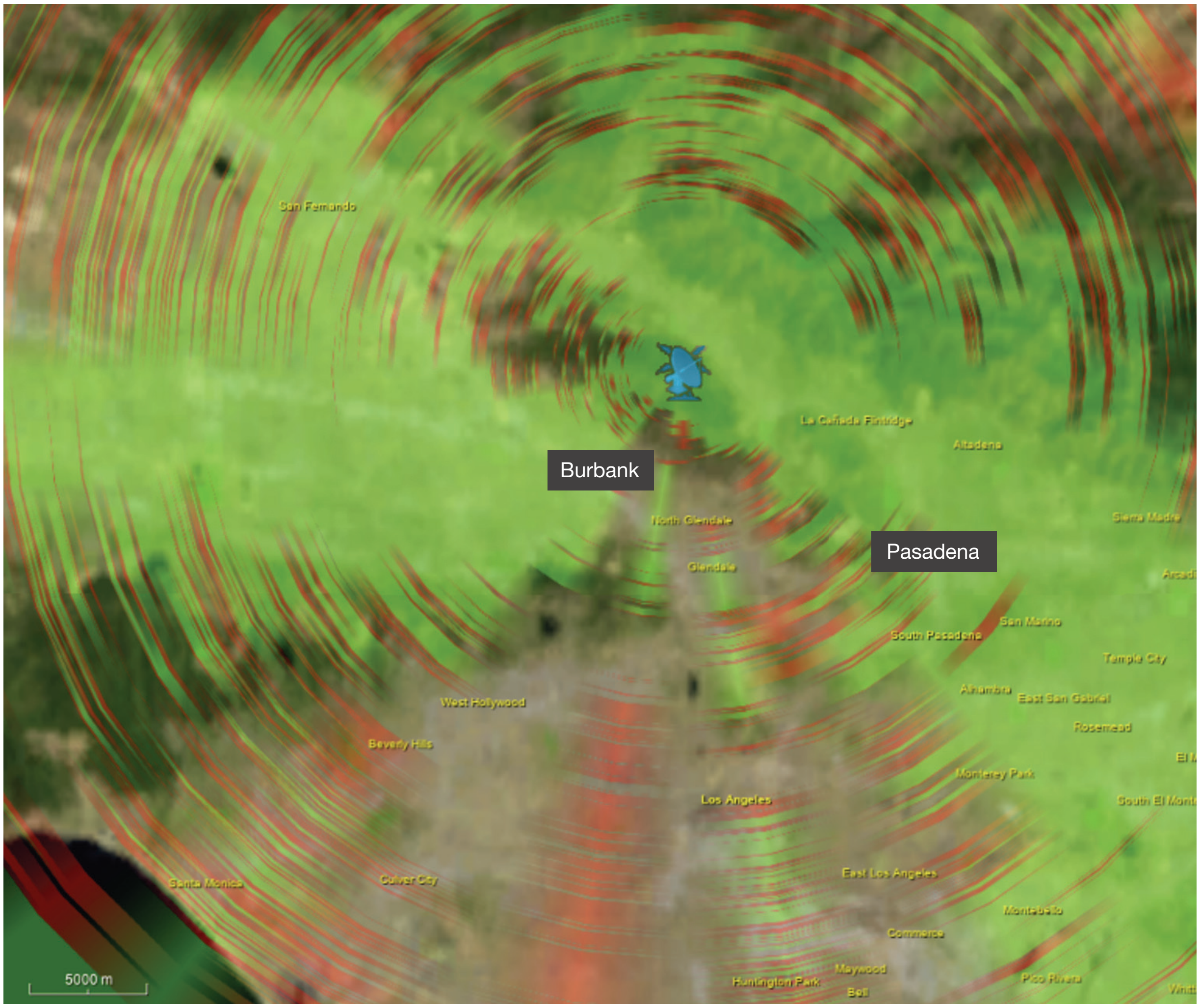


FIGURE B.8

25-W Land Mobile Radio/Project 25 Car Antenna, Broadcasting to Tower

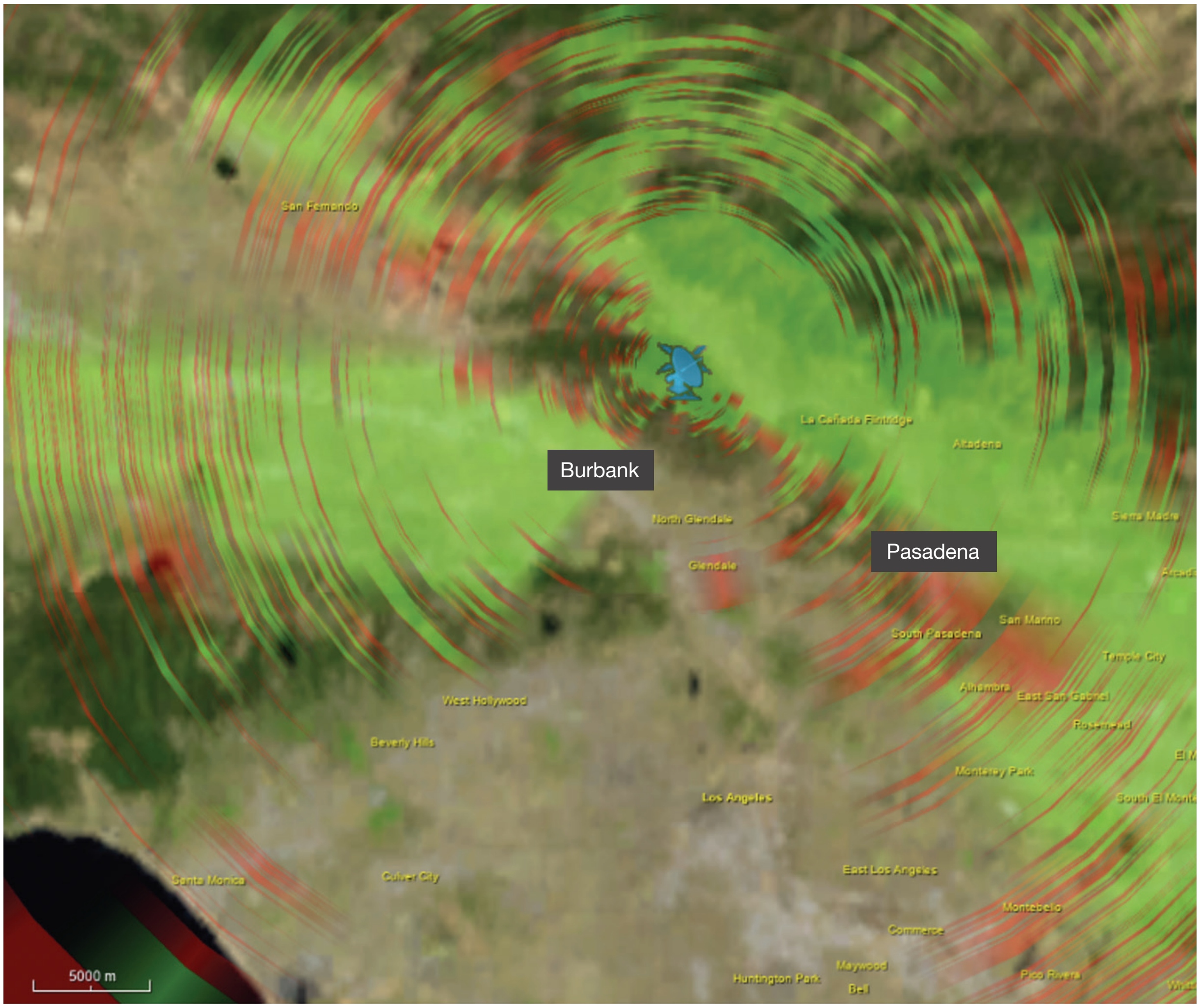
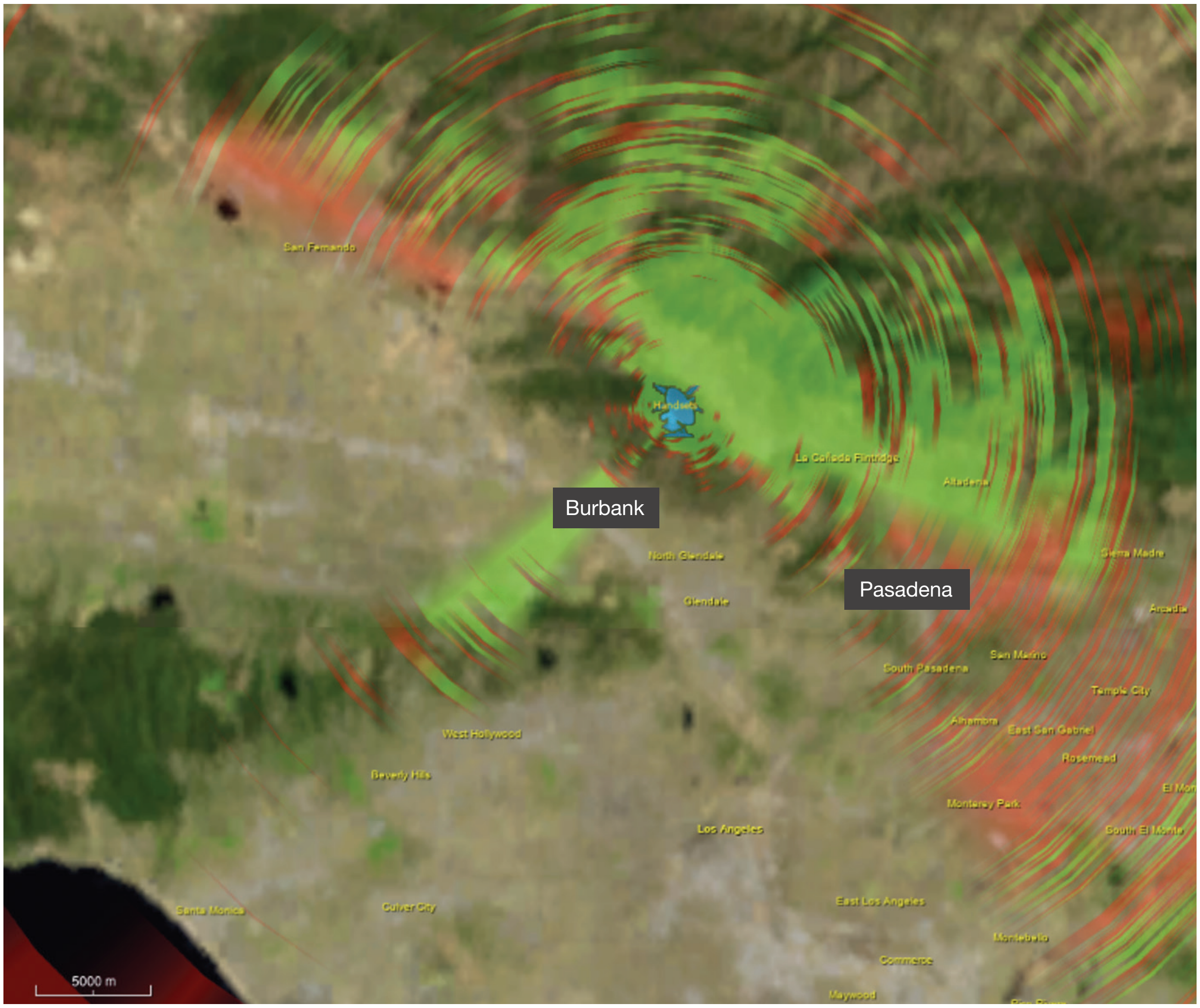


FIGURE B.9

25-W LMR/Project 25 Car Antenna, Car-to-Car Transmission



We see that, in all three cases, LMR/P25 outperforms all of the cellular examples. The coverage for the tower is significantly higher than for the car-to-tower case, but this option can still be useful for providing one-way communication of information. The car-to-car case also provides significantly improved coverage compared with the cellular examples. Note that this is true for direct point-to-point comparison of LMR versus cellular and does not take into account that cellular car-to-car networks can take advantage of multiple cell phone towers communicating from one area to the next. This case should be viewed as a comparison of LMR and cellular at the edge of cellular coverage in areas that do not have overlapping cellular coverage from multiple base stations.

APPENDIX C

Glossary

1G

The first generation of mobile voice communications. Created as an analog voice transmission technology.

2G

Second-generation mobile broadband; transition from analog to digital technology.

3G

Third-generation mobile broadband. Standardized the technology and facilitated the standardization process in the 3GPP collaborative; users saw enhanced video and audio speed, higher data transfer speed, and support for videoconferencing and web browsing.

4G

The fourth generation of mobile broadband, also known as Native internet protocol.

4G long-term evolution (4G LTE, or LTE)

The first iteration of 4G. LTE leveraged the dependability of data-optimized 3G broadband and delivered performance roughly equivalent to wired broadband. LTE is not necessarily 4G compliant.

5G

The emerging generation of mobile broadband technologies. Operates in low-, mid-, and high-band frequencies; adds significant speed and lower latency than previous generations.

5G Evolution (5G E)

A vendor term used by AT&T.

5G New Radio (5G NR)

3GPP standard set to fulfill the specs for 5G.

AT&T

The contract awardee to build, modernize, and manage the National Public Safety Broadband Network. Also referred to as FirstNet.com and AT&T/FirstNet.

Automatic vehicle locator

A device that uses GPS to remotely track the location of a vehicle.

COLT, COW, CSOW, SatCOLT

Terms used to describe mobile cell tower platforms that can be driven to a site ad hoc to provide broadband service where none exists or where the service is inadequate for the demand.

Cell on Wheels (COW)

A mobile cell tower platform, similar to a COLT (Cell on Light Truck), although usually smaller and more portable. A variant is *Cell on Wings*, an aerial platform used for the same purpose.

dBi	The forward gain of an antenna, measured in decibels.
dBm	An expression of power in decibels per milliwatt when measuring power emitted from amplifiers.
Emergency communications center (ECC)	The former name for *public safety answering point* or *public safety dispatch center.*
FirstNet	The name used to describe the National Public Safety Broadband Network.
FirstNet Authority	The governing body authorized by the creation of the National Public Safety Broadband Network. Oversees FirstNet.com to manage the development and operation of FirstNet as an independent authority within the U.S. Department of Commerce.
FirstNet.com	AT&T vendor site link, also known as FirstNet by AT&T.
First Responder Network Authority	Part of the creation of the National Public Safety Broadband Network. Formal name of FirstNet and the FirstNet Authority.
Mobile data terminal (MDT); mobile computer terminal	Most commonly a communications device or platform in police patrol vehicles, fire apparatuses, or similar first responder vehicles.
National Public Safety Broadband Network (NPSBN)	Also known as FirstNet.
Project 25 (P25)	Established in the United States in 1990, P25 establishes voluntary, consensus standards for interoperable land mobile radio systems.
P25 Phase II	Optimized narrowband communications to double the number of talk paths, doubling the number of logical channels available in the radio spectrum.
Public safety answering point (PSAP)	Usually a dispatch center for law enforcement or other first responders. See *emergency communications center (ECC).*
SAFECOM	An initiative formed in the aftermath of the 9/11, terrorist attacks to improve public safety interoperability and enhance public safety communications. A component of the Cybersecurity and Infrastructure Security Agency.
Unmanned aerial systems (UAS); unmanned aerial vehicles (UAVs); unmanned ground systems (UGS)	These can also be referred to as *drones*, *unpiloted aerial systems*, *unpiloted aerial vehicles*, *unpiloted ground systems*, or *robot systems.*

Abbreviations

3GPP	3rd Generation Partnership Project
5G E	5G Evolution
5G NR	5G New Radio
AGL	above ground level
APCO	Association of Public-Safety Communications Officials
CAD	computer-aided dispatch
CDMA	Code Division Multiple Access
CISA	Cybersecurity and Infrastructure Security Agency
COLT	Cell on Light Truck
COW	Cell on Wheels
CSOW	Cell Site on Wheels
DFR	Drone as First Responder
DSL	digital subscriber line
ECC	emergency communications center
EMS	emergency medical services
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FTE	full-time equivalent
GAO	U.S. Government Accountability Office
GB	gigabyte
GHz	gigahertz
GSM	Global System for Mobiles
HSPA	High-Speed Packet Access
IoT	Internet of Things
IP	internet protocol
IT	information technology
ITU	International Telecommunications Union
Kbps	kilobits per second
LA-RICS	Los Angeles Regional Interoperable Communications System
LMR	land mobile radio
LTE	Long-Term Evolution
LTE-A	Long-Term Evolution–Advanced
MAM	mobile application management
MB	megabyte
MBps	megabytes per second
MCPTT	Mission-Critical Push to Talk
MDM	mobile device management

MDT	mobile data terminal
MHz	megahertz
mmWave	millimeter wave
NCIC	National Crime Information Center
NG911	Next Generation 9-1-1
NIBRS	National Incident-Based Reporting System
NIJ	National Institute of Justice
NIST	National Institute of Standards and Technology
NPSBN	National Public Safety Broadband Network
NPSTC	National Public Safety Telecommunications Council
OTTPTT	over-the-top push to talk
P25	Project 25
PD	police department
POC	push to talk over cellular
PSAP	public safety answering point
PTT	push to talk
RFP	request for proposal
RIPA	Racial and Identity Profiling Act
RMS	records management systems
SatCOLT	Satellite Cell on Light Truck
SATCOM	satellite communications
UAS	unmanned aerial systems
UAV	unmanned aerial vehicle
UGS	unmanned ground systems
UGV	unmanned ground vehicle
UEM	unified endpoint management
UI	user interface
UMTS	Universal Mobile Telecommunications System
UX	user experience
WiMAX	Worldwide Interoperability for Microwave Access

References

3GPP, “GSM Spec History,” webpage, undated. As of July 9, 2022:
https://www.3gpp.org/specifications/gsm-history#fn1

———, “First 5G NR Specs Approved,” December 22, 2017. As of July 9, 2022:
https://www.3gpp.org/news-events/1929-nsa_nr_5

Adams, R. Dallon, “Super Bowl LV: Tech Titans Tap 5G, AR, and More to Boost Gameday Look and Feel,” TechRepublic, February 5, 2021.

Alleven, Monica, “T-Mobile Makes Public Safety a 3-Way Race—Sort Of,” Fierce Wireless, May 22, 2020.

———, “Verizon Beefs Up C-Band Deployment to 175M by End of 2022,” Fierce Wireless, March 3, 2022.

APCO International, “Next Generation 9-1-1,” webpage, undated a. As of July 9, 2022:
https://www.apcointl.org/technology/next-generation-9-1-1/

———, “P25 Organizational Overview and Committees,” webpage, undated b. As of July 9, 2022:
https://www.apcointl.org/technology/interoperability/project-25/p25-organizational-overview-and-committees/

AT&T, “Instant Communications for Enhanced Situational Awareness,” product brief for AT&T Enhanced Push-to-Talk for FirstNet, 2018. As of June 28, 2022:
https://www.firstnet.com/content/dam/firstnet/data-sheets/firstnet-att-enhanced-push-to-talk-data-sheet.pdf

———, “AT&T Delivers 5G & Networking Capabilities to Air Force Bases,” press release, Dallas, Tex., September 23, 2020.

“AT&T’s New Flying COW Drone to Be All-Weather Disaster Insurance,” All Things FirstNet, June 2, 2018.

Banse, Tom, “Wireless Carriers Deploy ‘Cell on Wheels’ to Boost Coverage in Eclipse Path,” Northwest News Network, August 14, 2017.

Basich, Melanie, “Wireless When You Need It,” *POLICE*, January 1, 2009.

Bostic, Mike, “FirstNet Flying COW™ Takes First Flight to Help Santa Clara County Sheriff Search & Rescue Stay Mission-Ready,” *AT&T Technology Blog*, December 3, 2019. As of July 11, 2022:
https://about.att.com/innovationblog/2019/12/fn_santa_clara_flying_cow.html

Bratcher, Jeff, “FirstNet Core Delivers on the Promise of a Dedicated Network for Public Safety,” blog post, FirstNet Authority, March 27, 2018. As of July 9, 2022:
https://www.firstnet.gov/newsroom/blog/firstnet-core-delivers-promise-dedicated-network-public-safety

BroadbandNow, “The Complete List of Internet Companies in the US,” web tool, undated. As of July 9, 2022:
https://broadbandnow.com/All-Providers

Brooks, Connor, *Local Police Departments: Policies and Procedures, 2016*, Washington, D.C.: Bureau of Justice Statistics, NCJ 254826, August 2020.

Brown, Sara, “5G, Explained,” MIT Sloan, February 13, 2020. As of July 9, 2022:
https://mitsloan.mit.edu/ideas-made-to-matter/5g-explained

Bureau of Justice Assistance, “Edward Byrne Memorial Justice Assistance Grant (JAG) Program: Fiscal Year 2019 Local Solicitation,” OMB No. 1121-0329, July 25, 2019.

Bureau of Justice Statistics, “Law Enforcement Management and Administrative Statistics (LEMAS),” webpage, undated. As of July 10, 2022:
https://bjs.ojp.gov/data-collection/law-enforcement-management-and-administrative-statistics-lemas#publications-0

Carter, Jeremy G., Eric Grommon, and Fred Franz, *Impact of Mobile Broadband Data Access on Police Operations: An Exploratory Case Study of One Medium-Sized Municipal Police Department: Final Report*, Rome, N.Y.: Engility Corporation, February 2014.

CISA—*See* Cybersecurity and Infrastructure Security Agency.

City of Albany, New York, "Request for Proposals for the Provision of Communications and Marketing Services," Albany, N.Y., RFP 2022-17, April 15, 2022. As of July 20, 2022:
https://albanyny.gov/DocumentCenter/View/7076/RFP-2022-17-Communications-and-Marketing-Services-ready-for-posting

City of Mequon, Wisconsin, "Request for Proposals (RFP): Information Technology Strategic Plan," Mequon, Wisc., March 10, 2021. As of July 20, 2022:
https://www.ci.mequon.wi.us/sites/default/files/fileattachments/community/page/22891/city_of_mequon_it_analysis_rfp_final.pdf

Criminal Justice Information Services Information Security Officer, *Criminal Justice Information Services (CJIS) Security Policy*, version 5.9, U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, June 1, 2020.

Cybersecurity and Infrastructure Security Agency, "Project 25 Resources," webpage, undated. As of July 9, 2022:
https://www.cisa.gov/safecom/p25

———, *National Emergency Communications Plan*, U.S. Department of Homeland Security, September 2019. As of July 9, 2022:
https://www.cisa.gov/sites/default/files/publications/19_0924_CISA_ECD-NECP-2019_0.pdf

———, "National Council of Statewide Interoperability Coordinators," webpage, last updated December 1, 2020. As of July 9, 2022:
https://www.cisa.gov/safecom/NCSWIC

Descant, Skip, "BRIEF: FirstNet to Receive $218M for 5G, Other Upgrades," Government Technology, June 17, 2020.

Douglas, Theo, "FirstNet Goes Local," *Government Technology*, September 2018.

Edson, Scott, "Creating the 'Connected Cop' Through a Broadband Network," National Institute of Justice, Office of Justice Programs, December 3, 2019. As of July 11, 2022:
https://nij.ojp.gov/topics/articles/creating-connected-cop-through-broadband-network

Electronics Notes, "WiMax IEEE 802.16 Technology Tutorial," undated. As of July 9, 2022:
https://www.electronics-notes.com/articles/connectivity/wimax/what-is-wimax-802-16-technology-basics.php

Engebretson, Joan, "Verizon to Introduce Frontline First Responder Network," Telecompetitor, March 5, 2021.

Favraud, Romain, Apostolos Apostolaras, Navid Nikaein, and Thanasis Korakis, "Toward Moving Public Safety Networks," *IEEE Communications Magazine*, Vol. 54, No. 3, March 2016, pp. 14–20.

"FBI Switches Remaining Operations from Verizon to FirstNet," *Government Technology*, December 8, 2020.

FCC—*See* Federal Communications Commission.

Federal Communications Commission, "800 MHz Spectrum," webpage, last updated September 17, 2018. As of July 9, 2022:
https://www.fcc.gov/general/800-mhz-spectrum

Federal Emergency Management Agency Grant Programs Directorate, *FEMA Preparedness Grants Manual*, version 2, Federal Emergency Management Agency, February 2021. As of July 11, 2022:
https://www.fema.gov/sites/default/files/documents/FEMA_2021-Preparedness-Grants-Manual_02-19-2021.pdf

———, *FEMA Preparedness Grants Manual*, version 3, Federal Emergency Management Agency, May 2022. As of July 10, 2022:
https://www.fema.gov/sites/default/files/documents/fema_fy-2022-preparedness-grants-manual.pdf

FEMA—*See* Federal Emergency Management Agency.

Finley, Klint, and Joanna Pearlstein, "The WIRED Guide to 5G," *Wired*, September 10, 2020.

FirstNet, "Rate Plans," webpage, undated. As of July 9, 2022:
https://www.firstnet.com/plans.html?tabs=26b46e66-b7ba-4c26-9bf8-63f88b12fb29

———, "More than 100 FirstNet ReadyTM Devices and 100 Approved Apps in the FirstNet App Catalog," December 17, 2019. As of July 9, 2022:
https://www.firstnet.com/community/news/firstnet-app-catalog.html

———, “FirstNet & 5G: An Experience Unlike Anything Else for America’s First Responders,” April 1, 2021.

FirstNet.gov, “FirstNet and Law Enforcement,” webpage, undated a. As of June 15, 2021:
https://www.firstnet.gov/resources/firstnet-and-law-enforcement

———, “History,” webpage, undated b. As of June 15, 2021:
https://firstnet.gov/about/history

———, “FirstNet Partners with AT&T to Build Wireless Broadband Network for America’s First Responders,” press release, Washington, D.C., March 30, 2017. As of June 15, 2021:
https://2014-2018.firstnet.gov/news/
firstnet-partners-att-build-wireless-broadband-network-americas-first-responders

“Flashback: What We Said About Mobile Phones in 1983,” CBS News, January 12, 2015.

Fussell, Sidney, “This AI Helps Police Monitor Social Media. Does It Go Too Far?” *Wired*, July 6, 2021.

Gallagher, Jill C., *Federal Grants and Loans for State and Local Emergency Communications Projects: Frequently Asked Questions*, Washington, D.C.: Congressional Research Service, R45213, updated September 20, 2018.

GAO—*See* U.S. Government Accountability Office.

Ghosh, Arunabha, Jun Zhang, Jeffrey G. Andrews, and Rias Muhamed, *Fundamentals of LTE*, Upper Saddle River, N.J.: Prentice Hall, 2011.

Griffith, David, “FirstNet and the Broadband Future,” *POLICE*, July 7, 2017.

Griffith, David, and Mark Clark, “Radios: Your Lifeline Is Evolving,” *POLICE*, June 22, 2014.

GSMA, *Network 2020: Mission Critical Communications*, London, 2017.

Harris, Kelly J., and William H. Romesburg, *Law Enforcement Tech Guide: How to Plan, Purchase and Manage Technology (Successfully!),* Washington, D.C.: U.S. Department of Justice, Office of Community Oriented Policing Services, August 2002.

Hightower, Satta Sarmah, “DSL vs. Cable vs. Fiber: The Big Three Broadband Technologies,” blog post, Frontier Communications, July 11, 2019. As July 11, 2022:
https://blog.frontier.com/2019/07/dsl-vs-cable-vs-fiber-broadband-internet-technologies/

Hildenbrand, Jerry, “How Much Mobile Data Does Streaming Media Use?” Android Central, August 10, 2020. As of April 26, 2021:
https://www.androidcentral.com/how-much-data-does-streaming-media-use

Hill, Kelly, “Key Takeaways from FirstNet’s Annual Report,” RCR Wireless News, March 3, 2021.

Hill, Simon, Simon Chandler, and Paula Beaton, “4G vs. LTE: The Differences Explained,” Digital Trends, October 21, 2021. As of July 11, 2022:
https://www.digitaltrends.com/mobile/4g-vs-lte/

Hollywood, John S., and Zev Winkelman, *Improving Information-Sharing Across Law Enforcement: Why Can’t We Know?* Santa Monica, Calif: RAND Corporation, RR-645-NIJ, 2015. As of June 27, 2022:
https://www.rand.org/pubs/research_reports/RR645.html

Hollywood, John S., Dulani Woods, Andrew Lauland, Sean E. Goodison, Thomas J. Wilson, and Brian A. Jackson, *Using Future Broadband Communications Technologies to Strengthen Law Enforcement*, Santa Monica, Calif.: RAND Corporation, RR-1462-NIJ, 2016. As of June 27, 2022:
http://www.rand.org/pubs/research_reports/RR1462.html

ICOM, “History of P25,” briefing slides, September 23, 2008. As of July 9, 2022:
icomamerica.com/en/landmobile/p25info/History_Of_P25_Program.pdf

Imel, Kathy J., and James W. Hart, *Understanding Wireless Communications in Public Safety: A Guidebook to Technology, Issues, Planning, and Management*, 2nd ed., National Law Enforcement and Corrections Technology Center, National Institute of Justice, January 2003.

Iridium, “Network,” webpage, undated. As of July 9, 2022:
https://www.iridium.com/network/

Jackman, Tom, “FirstNet, Broadband Network to Enable Police and Fire Responders to Talk to Each Other, Ready to Launch,” *Washington Post*, August 2, 2017.

Jackson, Donny, “Final Written Briefs Submitted in FirstNet Protest Case, Court to Determine Next Step,” Urgent Communications, February 16, 2017.

———, “FirstNet One LTE Blimp Used for First Time in Aftermath of Hurricane Laura,” Urgent Communications, September 23, 2020.

———, “Verizon Calls On Industry to Provide ‘True Interoperability’ to First-Responder Community,” Urgent Communications, January 25, 2021a.

———, “FirstNet Adoption Tops 15,000 Agencies, 1.9 Million Connections, AT&T Says,” Urgent Communications, January 29, 2021b.

———, “FirstNet Exceeds 3 Million Connections and 19,500 Agencies, AT&T Reports,” Urgent Communications, January 26, 2022.

Jackson, Donny, and Andy Castillo, “PTT over FirstNet Gains Traction, with Some Entities Planning to Abandon LMR,” Urgent Communications, March 24, 2022.

Johnson, Brian, “Take a Rare Look Inside Verizon’s Secret Disaster-Relief Cave,” KMBC News, last updated May 20, 2018.

Level Education, “Smartphones: A Supercomputer in Your Pocket,” Medium, April 21, 2016.

Koh, Racheal, “4G vs. LTE: In-Depth Guide to Its Differences,” Cellularnews.com, last updated December 18, 2020. As of July 11, 2022:
https://cellularnews.com/cellular-network/4g-vs-lte-in-depth-guide-to-its-differences/

Kozlowski, Jonathan, “Spotlight On: Verizon,” Officer.com, July 10, 2020. As of July 11, 2022:
https://www.officer.com/command-hq/technology/communications/article/21143122/spotlight-on-the-verizon-public-safety-communications-network

Kramer, Amber, “Expanding High-Demand Network Coverage with Cows,” blog post, CellSite Solutions, LLC, May 10, 2017. As of July 11, 2022:
https://cellsitesolutions.com/cell-on-wheels-expand-network-coverage/

Lastovetska, Anastasiia, “App Development Cost: Understand Your Budget to Build Powerful Apps,” *MLSDev Blog*, June 30, 2022. As of July 11, 2022:
https://mlsdev.com/blog/app-development-cost

Mack, Eric, “The First Commercial Cell Call Was Made 30 Years Ago on a $9,000 Phone,” *Forbes*, October 13, 2013.

Matyunina, Julia, “Top 7 Biggest Hidden Costs of Mobile App Development,” blog post, Mobindustry, November 24, 2021. As of July 11, 2022:
https://www.mobindustry.net/top-7-biggest-hidden-costs-of-mobile-app-development/

McCallion, Jane, “LTE vs 4G: What Is LTE and 4G and Which Is Better?” ITPro, June 21, 2022. As of July 11, 2022:
https://www.itpro.com/mobile/28690/lte-vs-4g

McHugh, Brendon, “Public-Safety Broadband Applications and Benefits,” *MissionCritical Communications*, February 18, 2022.

Mirgon, Richard, “Verizon Just Can’t Help Themselves!” All Things FirstNet, December 8, 2019.

Mobile Solutions Services, “Managing Your Mobile Devices: Are You Getting Your Money’s Worth?” white paper, Centennial, Colo.: December 2014.

Monopoli, Daniel M., “Mobile Data Terminals: Past, Present and Future,” in Richard Scherpenzeel, ed., *Computerization in the Management of the Criminal Justice System*, Helsinki and The Hague: European Institute for Crime Prevention and Control and Ministry of Justice of the Netherlands, 1996, pp. 289–294.

National 911 Program, *NG911: A Guide for Law Enforcement Officials*, undated. As of July 9, 2022:
https://www.911.gov/projects/ng911-for-public-safety-leaders/ng911-guide-for-leaders-in-law-enforcement/

National Institute of Standards and Technology, “Low-Cost NIST Demo Links Public Safety Radios to Broadband Wireless Network,” news release, April 12, 2021.

National Public Safety Telecommunications Council, *Defining Public Safety Grade Systems and Facilities: Final Report*, Littleton, Colo.: May 22, 2014.

———, *Public Safety Land Mobile Radio (LMR) Interoperability with LTE Mission Critical Push to Talk: Final Report*, Littleton, Colo.: January 8, 2018.

New England Radio Consultants, LLC, "Town of East Windsor Connecticut: Qualifications & Proposal for a LMR Analysis Land Mobile Consultant," request for proposal, Shelton, Conn., February 19, 2021. As of July 20, 2022:
https://www.eastwindsor-ct.gov/sites/g/files/vyhlif4381/f/pages/east_windsor_nerc_consulting_proposal.docx_0.pdf

Newman, Daniel, "Five Advancements 5G Will Enable in the Future," *Forbes*, March 6, 2019.

Nilsson, Jeff, "Albert Einstein: 'Imagination Is More Important Than Knowledge,'" *Saturday Evening Post*, March 20, 2010.

NIST—*See* National Institute of Standards and Technology.

NPSTC—*See* National Public Safety Telecommunications Council.

P25, "More Information About P25 Phase 2," webpage, undated. As of July 11, 2022:
http://www.p25phase2.com/p25-phase-2

Oxford Economics, *Maximizing Mobile Value: Is BYOD Holding You Back?* June 2018.

Parkinson, Edward, "FirstNet Is Interoperability," blog post, FirstNet.gov, October 29, 2020. As of July 11, 2022:
https://firstnet.gov/newsroom/blog/firstnet-interoperability

Paulson, Anna, and Thomas Schwengler, "A Review of Public Safety Communications, from LMR to Voice Over LTE (VoLT E)," *2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, London: IEEE, 2013, pp. 3513–3517.

Public Law 112-96, Middle Class Tax Relief and Job Creation Act of 2012, February 22, 2012.

Project 25 Technology Interest Group, "The Benefits of Project 25," April 2016. As of July 11, 2022:
https://project25.org/images/stories/ptig/Benefits_of_P25_Final_April_2016_REV_02_160407.pdf

Qualcomm, "5GNR," webpage, undated. As of July 11, 2022:
https://www.qualcomm.com/research/5g/5g-nr

———, "The Evolution of Mobile Technologies 1G > 4G LTE," June 2014.

Reed, Brad, "A Brief History of Smartphones," PC World, June 18, 2010.

Remmert, Harald, "2G, 3G, 4G LTE Network Shutdown Updates," *Digi Blog*, June 8, 2021. As of July 11, 2022:
https://www.digi.com/blog/post/2g-3g-4g-lte-network-shutdown-updates

Ryan, Camille, *Computer and Internet Use in the United States: 2016*, Washington, D.C.: U.S. Census Bureau, ACS-39, August 2018.

SAFECOM, *Office of Emergency Communications: Fiscal Year 2015 SAFECOM Guidance on Emergency Communications Grants*, Washington, D.C.: U.S. Department of Homeland Security, 2015.

———, "Release of the Emergency Communications Governance Guide for State, Local, Tribal, and Territorial Officials," *SAFECOM Blog*, last revised April 22, 2020. As of July 21, 2022:
https://www.cisa.gov/safecom/blog/2015/09/24/release-emergency-communications-governance-guide-state-local-tribal-and

———, *Interoperability Continuum: A Tool for Improving Emergency Response Communications and Interoperability*, Washington, D.C.: U.S. Department of Homeland Security, June 2021.

SAFECOM and National Council of Statewide Interoperability Coordinators, *Emergency Communications Governance Guide for State, Local, Tribal, and Territorial Officials*, Washington, D.C.: Cybersecurity and Infrastructure Security Agency, 2018.

Salmensuu, Simo, "Security and the Bottom Line: The ROI of Mobile Device Management," *Security*, July 16, 2019.

Sambar, Chris, statement presented before the U.S. House of Representatives Committee on Energy and Commerce Subcommittee on Communications and Technology on November 1, 2017, Washington, D.C., 2017. As of June 27, 2022:
https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Testimony-Sambar-CAT-Hrg-on-Oversight-of-FirstNet-State-Perspectives-2017-11-01.pdf

———, "Reaching New Heights in Network Disaster Recovery," *AT&T Technology Blog*, December 3, 2019. As of July 9, 2022:
https://about.att.com/innovationblog/2019/12/fn_flying_cows.html

Segan, Sascha, "5G vs. 5G E vs. 5GHz: What's the Difference?" *PCMag*, January 7, 2019.

———, "CDMA vs. GSM: What's the Difference?" *PCMag*, April 7, 2020.

———, "What Is 5G?" *PCMag*, updated May 16, 2022.

Seybold, Andrew M., *Push-to-Talk over Cellular: Integrated LTE and LMR Communication Success in the Mainstream*, Phoenix, Ariz.: Andrew Seybold, Inc., March 13, 2017a.

———, "Public Safety Advocate: Public Safety Grade," All Things FirstNet, September 14, 2017b. As of July 20, 2022:
https://allthingsfirstnet.com/public-safety-advocate-public-safety-grade/

Shepardson, David, and Jeffrey Dastin, "U.S. Drone Program Taps Apple, Passes over Amazon, China's DJI," Reuters, May 9, 2018.

Silver, Laura, "Smartphone Ownership Is Growing Rapidly Around the World, But Not Always Equally," Pew Research Center, February 5, 2019.

Spector, Dina, "What Is WiMax? And How Does It Work?" *Business Insider*, September 23, 2010.

State of California, Racial and Identity Profiling Act of 2015, Assembly Bill No. 953, *Legislative Counsel's Digest*, Ch. 466, October 3, 2015. As of July 9, 2022:
https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201520160AB953

Stevenson, Ryan A., David Fotheringham, Tom Freeman, Turner Noel, Tim Mason, and Shahram Shafie, "High-Throughput Satellite Connectivity for the Constant Contact Vehicle," *2018 48th European Microwave Conference (EuMC)*, IEEE, 2018, pp. 316–319.

Stockton, Dale, "How Police Departments Can Win Grants for Mobile Technology Projects," Insights by Samsung, January 31, 2019. As of August 4, 2022:
https://insights.samsung.com/about/

Techopedia, "Cell on Wheels (COW)," technology dictionary entry, undated. As of October 13, 2020:
https://www.techopedia.com/definition/26001/cell-on-wheels-cow

Todd, Zoe, Sydney Trattner, and Jane McMullen, "Ahead of Camp Fire Anniversary, New Details Emerge of Troubled Evacuation," PBS *Frontline*, October 25, 2019.

"U.S. Army Selects FirstNet, Built with AT&T, for Public Safety Communications Across 72 Installations in the U.S.," TMCNet.com, October 12, 2020. As of July 11, 2022:
https://www.tmcnet.com/usubmit/-us-army-selects-firstnet-built-with-att-public-/2020/10/12/9235883.htm

U.S. Geological Survey, "State of California Department of Water Resources: Burbank Quadrangle," topographic map, 1966. As of July 11, 2022:
https://pw.lacounty.gov/sur/nas/landrecords/CETopo/QuadSheets/BURBANK.pdf

U.S. Government Accountability Office, "Decision," T-Mobile USA, Inc., File B-418394, April 8, 2020. As of June 28, 2022:
https://www.gao.gov/assets/b-418394.pdf

———, *Public-Safety Broadband Network: Congressional Action Required to Ensure Network Continuity*, Washington, D.C., GAO-22-104915, February 2022.

U.S. House of Representatives, a bill to amend the Middle Class Tax Relief and Job Creation Act of 2012 to reauthorize the First Responder Network Authority, 117th Congress, H.R. 6768, introduced February 18, 2022.

"Utah Police Look to Artificial Intelligence for Assistance," *Salt Lake Tribune*, January 14, 2020.

Van Grove, Jennifer, "U.S. Government Picks San Diego to Test Autonomous Drone Deliveries," *San Diego Union Tribune*, May 9, 2018.

Verizon, "VerizonFrontline," webpage, undated. As of July 11, 2022:
https://www.verizon.com/business/solutions/public-sector/public-safety/

———, comments before the Department of Commerce in the Matter of National Telecommunications and Information Administration Development of the Nationwide Interoperable Public Safety Broadband Network—FirstNet NOI, Washington, D.C., Docket No. 12092850-2505-01, RIN 0660-XC002, November 9, 2012. As of June 28, 2022:
https://www.ntia.doc.gov/files/ntia/verizon_firstnet_comments_11-9-2012.pdf

———, "Verizon to Build Dedicated Network Core for Public Safety," press release, New York, August 16, 2017.

———, "Verizon Unveils Public Safety Private Core," press release, New York, March 27, 2018.

———, "What Is the Difference Between 3G, 4G and 5G?" November 18, 2019. As of July 9, 2022:
https://www.verizon.com/about/our-company/5g/difference-between-3g-4g-5g

———, "Verizon Launches Verizon Frontline with Pro Basketball Partnerships," press release, Atlanta, Ga., March 4, 2021.

"Verizon Launches Public Safety Advisory Council Event Series," *Government Technology*, August 3, 2020.

Wagner, Arthur, "Legislatures Require Police Body Camera Use Statewide," National Conference of State Legislatures, April 30, 2021. As of July 11, 2022:
https://www.ncsl.org/research/civil-and-criminal-justice/
legislatures-require-police-body-camera-use-statewide-magazine2021.aspx

Wendelken, Sandra, "AT&T to Pay $14.5 Million, Provide 3,300 Devices for LA-RICS LTE Network," *MissionCritical Communications*, December 13, 2017.

"When Is 5G Coming to You? The Definitive Guide to the 5G Network Rollout," Tom's Guide, April 29, 2021. As of July 11, 2022:
https://www.tomsguide.com/special-report/
when-is-5g-coming-to-you-the-definitive-guide-to-the-5g-network-rollout

RAND SOCIAL AND ECONOMIC WELL-BEING

In 2018, law enforcement agencies gained access to a federally funded and managed, interoperable first responder broadband communications network, the Nationwide Public Safety Broadband Network (NPSBN), known as FirstNet. FirstNet was supposed to result in simple solutions for agencies seeking interoperability. For various reasons, this has not happened. Every law enforcement and first responder agency has legacy systems and equipment for mobile broadband uses and is faced with a complex set of decisions about its broadband communications infrastructure. Several competitors to FirstNet have emerged and are competing for a share of the public safety broadband market, causing confusion for end users. In addition, to make decisions regarding broadband communications systems, many agencies need assistance to understand the technical differences between various options.

To address the dizzying array of providers, capabilities, and options for the future, RAND researchers developed practical knowledge to inform agencies about available broadband options and opportunities, governance issues, funding options, costs, and barriers to implementation. This report is intended to help law enforcement executives, their staff, and their city or county communications technology providers chart a course forward that optimizes the systems they have now while better integrating technologies for enhanced interoperability.

$36.00

ISBN-10 1-9774-0992-X
ISBN-13 978-1-9774-0992-8

53600

9 781977 409928

www.rand.org

RR-A2019-1