Toward A Next Generation Architecture For Public Safety Communications

Philip J. Weiser
School of Law and
Interdisciplinary Telecommunications Program
University of Colorado Boulder, CO 80309-0530
Phil.Weiser@colorado.edu

Dale N. Hatfield
Interdisciplinary Telecommunications Program
University of Colorado Boulder, CO 80309-0530
Dale.Hatfield@ieee.org

Brad Bernthal
School of Law and
Interdisciplinary Telecommunications Program
University of Colorado Boulder, CO 80309-0530
Brad.Bernthal@colorado.edu

Abstract – **In the aftermath of Hurricane Katrina, a unitary reliance on Land Mobile Radio systems (LMRs) failed public safety agencies, leaving them without any source of communications once they lost transmission capability. Unfortunately, in the wake of this tragedy, many have dusted off traditional prescriptions for improving public safety communications, such as more dedicated spectrum and more money for single-purpose LMRs (or LMRs based on technology that fails to facilitate broader functionalities). As we explain, however, both the needs underscored by Katrina and the capabilities made possible by emerging technologies call for a different strategy.**

In this paper, we argue that sound policy favors adoption of a next generation *flexible architecture* strategy for public safety communications. Such a flexible architecture embraces technological convergence and, accordingly, strives to coordinate existing LMRs, commercial terrestrial services, satellite technology, and wireless broadband systems to provide a robust, reliable, secure, and interoperable broadband communications system. Additionally, this approach would take advantage of "multi-mode" radios which are already a reality in most segments of the marketplace (except for public safety). Such multi-mode radios are expected to be even more robust once the recently authorized "ancillary terrestrial component" (ATC) of mobile satellite services becomes an option for public safety agencies.

Notably, the flexible architecture that we advocate does not necessarily require additional spectrum dedicated for public safety agencies nor prohibitive financial investment in the equipment needed to use spectrum effectively. Rather, public safety agencies can leverage networks provided by commercial providers—particularly hybrid satellite and terrestrial systems—to satisfy many public safety needs in a cost-effective fashion. To advance this vision, policymakers should ensure that (1) satellite and terrestrial providers are afforded the opportunity—through pro-market and innovative spectrum policies—to develop effective offerings for public safety agencies; and (2) public safety agencies receive sufficient financial support to promote this type of a hybrid, next generation architecture.

I. INTRODUCTION*

In light of the tragic events and aftermath of Hurricane Katrina, increased attention has focused on how policymakers should respond to rising concerns about deficiencies in public safety communications systems. The communication breakdowns in the wake of Katrina reflected concerns that *pre-existed* Katrina—i.e., the relevant public safety agencies lacked interoperable, redundant, secure, and economic methods of communicating with one another. Unfortunately, in the

* A prior version of this paper, "Learning From The Hurricane Katrina Disaster: A Strategy for the Next Generation of Public Safety Communications," was published as a white paper commissioned by Mobile Satellite Ventures.

wake of this tragedy, many have advocated the traditionally recommended prescriptions for improving public safety communications (i.e., more dedicated spectrum and more money for single-purpose Land Mobile Radio Systems (LMRs)). As we explain, however, both the needs underscored by Katrina and the capabilities made possible by modern technology suggest a next generation strategy of a *flexible architecture*. Such an architecture takes advantage of technological advances and incorporates traditional LMRs along with satellite, terrestrial, and wireless broadband systems.[1] Additionally, we argue that by embracing a flexible architecture, public safety agencies can rely on services provided by commercial providers—particularly hybrid satellite and terrestrial systems—and thereby satisfy many of their needs cost-effectively.[2]

The flexible architecture we advocate is one that will almost certainly be available before the completion of the digital transition and the availability of more spectrum for public safety agencies. In particular, the concept of "multi-mode" radios is already a widespread reality in most segments of the marketplace (except for public safety).[3] Such multi-mode radios are expected to be even more robust once the recently authorized "ancillary terrestrial component" (ATC) of mobile satellite services becomes an option for public safety agencies. Even using traditional satellite technology, firms are able to provide service to a number of public safety agencies today. But beginning within the next couple of years, after completing the deployment of an ATC service, firms are expected to be able to expand this service and offer it more efficiently to public safety agencies across the United States and provide it as a critical part of a realistic and effective nationwide interoperable broadband mobile communications system for public safety agencies. Such a convergence between wireless and satellite is already becoming a reality in other countries, such as South Korea, meaning that its prospects in the U.S. will depend on whether the market appreciates the benefits of a built-in satellite backup, not on whether the product is technically feasible.[4]

This article proceeds in five parts. Following this Introduction, Part II reviews the events around Hurricane Katrina and underscores how public safety communications systems failed to operate effectively in its aftermath. Part III outlines the requirements for an ideal public safety network, noting the often cited shortcomings of traditional commercial providers. Part IV explains how public safety agencies can utilize networks provided by commercial providers—particularly hybrid satellite and terrestrial systems—to satisfy the relevant requirements in a cost-effective fashion. Finally, Part V considers how policymakers can facilitate the transition to such optimal hybrid networks.

II. Katrina and Its Lessons

The aftermath of Hurricane Katrina, when many mission critical networks were down and unavailable to key governmental officials and first responders, made clear that effective communication during a crisis should not and cannot be a luxury. Significantly, while tragic, Katrina's communication breakdowns were foreseeable and in some respects mirrored similar communication deficiencies that frustrated responses to previous major incidents such as the Columbine High School shootings and the terrorist attack on the World Trade Center.[5] The lesson of these events are plain: when mission critical networks do not live up to their name—i.e., are not reliable, survivable, and secure—first responders are left unable to perform their job effectively. In the case of Katrina, public safety agencies realized that traditional Land Mobile Radio Systems (LMRs)—even along with commercial wireless systems—are unlikely to remain widely available under certain adverse conditions. As Federal Communications Commission (FCC) Chairman Martin emphasized, "[i]f we learned anything from Hurricane Katrina, it is that we cannot rely solely on terrestrial communications."[6]

As many accounts have reported, Hurricane Katrina left Louisiana's governmental communications systems in shambles. Governor Kathleen Blanco reported early on that wireless networks throughout the state were down and that many state officials were cut off from communicating with one another. As Reuters put it, "[t]he collapse of the communications network in the New Orleans area has been widely blamed for contributing to the disaster there, as local officials

[1] *See*, *e.g.,* Linda K. Moore, *Public Safety Communications: Policy, Proposals, Legislation and Progress*, CRS Report for Congress 17 (June 2005) (http://www.fas.org/sgp/crs/homesec/RL32594.pdf) (stating that advanced communication technology is "typified by the near-ubiquity of the Internet and the wide availability of advanced wireless telephone" services, suggesting the possibility of "a world of end-to-end communications for public safety").

[2] In a recent Federal Communications Commission (FCC) Report to Congress, the FCC suggested that "there may now be a place for commercial providers to assist public safety in securing and protecting the homeland." *FCC Report to Congress: On the Study to Assess Short-Term and Long-Term Needs for Allocations of Additional Portions of the Electromagnetic Spectrum for Federal, State and Local Emergency Response Providers,* 2005 WL 3618426 at ¶ 2 (F.C.C.)(December 19, 2005). Other commentators have expressed similar views concerning the need to consider and better utilize commercial systems. *See, e.g.,* Jon M. Peha, *Protecting Public Safety With Better Communications Systems*, IEEE Communications Magazine (March 2005) (http://www.comsoc.org/ci1/Public/2005/Mar/cireg.html) (stating that "the United States should reevaluate the traditional separation between public safety systems and commercial systems").

[3] *See, e.g.*, Mike Dano, *LG, Qualcomm Release Dual-Mode Technology*, RCR Wireless News (September 23, 2005) (www.rcrnews.com/printwindow.cms?newsId=24251&pageType=news) (discussing latest multi-mode technological developments).

[4] Katrina Could Unite Wireless, Satellite Industries, Communications Daily (September 22, 2005).

[5] *See* William Pessemier, *Top Priority: A Fire Service Guide to Interoperable Communications*, 2 (International Association of Fire Chiefs 2005) (warning prior to Hurricane Katrina that despite "numerous after-action reports, public safety services have yet to make significant progress in comprehensively addressing interoperability.").

[6] Statement of Kevin J. Martin, Hearing on Communications in A Disaster 7 (September 22, 2005).

were unable to talk to each other and to federal authorities to arrange relief in the days after Katrina laid waste to the city."[7]

As failed communications networks emerged as an Achilles' heel of first responder efforts, some bright spots emerged from services generally underutilized in public safety communications such as satellite units that remained effective throughout the tragedy and non-traditional service providers (such as Wireless Internet Service Providers (WISPs)). Keith Sims, the telecom chief of Tampa Electric who brought a team to New Orleans to repair the damage, explained that "[c]ellphones don't do much good after a hurricane" whereas satellite units worked very well in the storm's aftermath. As another user of satellite technology put it, "it's the only way [our employees] can talk to one another."[8] Noting that satellite systems remained intact during the crisis, FCC Chairman Martin explained that they "helped to bridge the gaps left by outages by providing satellite phones and video links to law enforcement, medical personnel, emergency relief personnel, and news outlets."[9] In addition, WISPs also proved helpful in Katrina's wake by restoring coverage in over 400 affected locations.[10] WISPs were particularly valuable because of their speed: they were able to assist the Federal Emergency Management Agency (FEMA), state and local police by deploying networks spanning several miles in just one to two days.[11]

The assistance offered by mobile satellite services to governmental organizations in the affected areas included access to reliable, quality communications for agencies ranging from the American Red Cross, FEMA, and the Louisiana Department of Homeland Security. Summing up the situation, one trade publication explained that "[a]fter Hurricane Katrina wreaked havoc on the Gulf Coast terrestrial wireless network, satellite phones and satellite data services played a critical role in filling communication gaps left by the storm."[12] Indeed, some Louisiana officials have been sharply criticized for a "penny wise-pound foolish" decision to discontinue satellite phone service in parishes' emergency management offices in 2004.[13] Rather than pay the $65 monthly service fee, all but a few parishes returned their satellite phones after the state stopped using federal funding to pay the fees. After Katrina struck, however, satellite turned out to be the sole means of communication for some affected areas, so the state had to send the phones back.[14]

Communications network failures in Katrina resulted from weaknesses that included interoperability, reliability, and survivability shortcomings. With respect to interoperability, a frequently lamented problem in the United States is the fractured nature of communications systems between different jurisdictions as well as variance in systems used by different providers *within* the same jurisdiction. As one expert has noted, the United States "has never developed a coherent architecture for public safety communications infrastructure, nor even a meaningful national strategy that would lead to close coordination of the more than fifty thousand US public safety agencies towards a commonly accepted set of objectives."[15] On this score, leaders have expressed skepticism on the prospects of a near term interoperability fix across jurisdictions for the existing public safety communications infrastructure.[16] David Boyd, director of the Department of Homeland Security's Office for Interoperability and Compatibility, recently testified that he believes that a dramatic change in interoperability would not occur in the next three years and, indeed, under "perfect conditions" such a change in communications systems will take at least 5 to 10 years.[17]

With respect to reliability and survivability, a central lesson underscored by Katrina is that relying solely on Land Mobile Radios (LMRs) does not provide the reliability and survivability sometimes suggested by its boosters. In particular, some have claimed that governmental systems that are maintained by public safety agencies are more robust than commercial systems insofar as they are protected in ways that commercial networks are not and, accordingly, they are better able to operate during an emergency. Such claims, however, generally focus on a particular threat—traffic from ordinary users overwhelming the network. Other claims about commercial systems—say, the need to provide backup power, enable re-charging of the handsets, and the lack of coverage in some areas—may prove problematic in certain cases. None-

[7] Wireless Carriers Reconnect in New Orleans, CNET News.com (September 4, 2005) (http://news.com.com/Wireless+carriers+reconnect+in+New+Orleans/2100-1039_3-5849066.html); *see also* Mimi Hall, *Hard Lessons of Katrina Being Put to Immediate Use*, USA Today 1A (September 22, 2005) ("When Katrina wiped out communications along the Gulf Coast, officials and key emergency workers were cut off from each other. That contributed greatly to the chaos on the ground.").

[8] Paul Davidson, Satellite phones provide critical link to outside world, USA Today (September 5, 2005) (http://www.usatoday.com/tech/wireless/2005-09-05-satellite-phones_x.htm?POE=TECISVA); *see also* Press Release, State Wildlife Agency Playing Large Role in Hurricane Relief (September 6, 2005) (http://www.mdwfp.com/Level1/NewsRoom.asp?ID=302) (explaining that satellite units provided a critical means of communicating with one another, enabling different relief efforts to work together).

[9] *See, e.g.*, Statement of Kevin J. Martin, *supra* note 6 at 3; *see also* Presentation of Kenneth Moran, Director, Office of Homeland Security, Enforcement Bureau Agenda Meeting of the Federal Communications Commission (September 15, 2005) (http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-261112A1.pdf).

[10] *See* Presentation of Kenneth Moran, *supra* note 9.

[11] *Id.*

[12] Katrina Could Unite Wireless, *supra* note 4.

[13] *See* United States House of Representatives, *A Failure of Initiative: The Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina* 173, 178 (February 15, 2006) (http://www.c-span.org/pdf/katrinareport.pdf).

[14] *Id.*

[15] John Peha, *How America's Fragmented Approach to Public Safety Wastes Money and Spectrum*, 2, presented at 33rd Telecommunications Policy Research Conference (September 2005) (http://web.si.umich.edu/tprc/papers/2005/438/Peha_Public_Safety_Communications_TPRC_2005.pdf).

[16] This of course is not to suggest that all public safety communications infrastructure is of recent vintage. Indeed, Katrina brought attention to the advancing age of certain systems, including many proprietary systems still in use that are 30 or more years old. *See* United States House of Representatives, *A Failure of Initiative*, *supra* note 13, at 174.

[17] House Democrats Criticize FCC, Administration on Public Safety Interoperability Efforts, TR Daily (April 15, 2006).

theless, an optimally designed system (i.e., a flexible one allowing the use of satellite technology and multiple networks) can provide the greatest assurance that public safety communications will remain available during a time of crisis.

In short, it is essential that mission critical networks be able to survive natural or manmade disasters so that first responders can perform their role effectively. Katrina reminds us that LMR systems can be destroyed even when protected by some measures not used by their commercial brethren, underscoring that the best assurance of survivability is the use of a flexible and diverse system that includes satellite technology. As we discuss in Part III, the flexibility and redundancy of system that includes satellite technology is only one of a number of requirements that we believe are important for a next generation public safety communications system.

III. Requirements For A Next Generation Public Safety Communications System

In the wake of 9/11, Katrina, and an emerging awareness of the shortcomings of current public safety communications networks, most policymakers are familiar with the arguments for developing a next generation (i.e., broadband and interoperable) mobile radio network. Thus, rather than focus on the particular applications and rationale for such a network, this Part explains the key requirements of any such network. In particular, we explain the need for (A) ubiquitous access; (B) reliability; (C) interoperability; (D) configurability; and (E) security. In so doing, we make a special effort to acknowledge the criticisms traditionally leveled at commercial wireless providers.

A. Ubiquitous Access

The fundamental requirement for public safety mobile radio networks is that they must function in all areas served by first responders. The need for ubiquitous access is a notorious shortcoming of modern commercial mobile radio networks, which often do not serve more remote areas.[18] As commercial providers underscore, the territory they do serve often includes 90% of the population. Because of the increasingly urbanized nature of the nation, however, this coverage can be achieved while covering less than 10% percent of the U.S. land area. Given this limited geographic reach and the lack of coverage for the other 10% of the population, public safety agencies traditionally have eschewed reliance on commercial systems and have developed their own land mobile radio (LMR) systems. Significantly, even many LMR systems operated by public safety agencies do not cover their entire territory. The New Mexico State Police's system, for example, cannot reach 15% of the state—and is limited to voice communications.[19]

The second aspect of ubiquitous coverage involves ensuring service in buildings. Historically, the inability of radio communications to adequately perform within buildings represented a notable failing of public safety LMRs—and one that has led to tragic results during emergency situations such as 9/11.[20] To respond to this failing, some cities have required in-building coverage plans as part of any new construction (such as the installation of bi-directional amplifiers). In-building systems can be expensive, however, with major high rise buildings requiring an investment of $1-$2 million.[21]

B. Reliability

For public safety agencies, the second critical requirement is that "mission critical" networks be able to survive and continue to operate during natural or man-made disasters, such as hurricanes, earthquakes, fires, or a high-powered blast caused by a bomb. Not surprisingly, perhaps the greatest challenge for public communications systems to surmount is to provide adequate service in the absence of electrical power. "A well-planned and robust emergency communications system," a recent congressional report explained, "should be sustainable at reasonable levels even after electrical power is lost."[22] In many cases, traditional commercial networks are not engineered to withstand such disasters—either because they are not protected or because they do not have sufficient generation capacity or battery back-up to stay online if the power grid goes down. Moreover, even if available, commercial systems are often overloaded by calls during emergencies; as one report explained, "[e]xperience has shown that such systems are often the most unreliable during critical incidents when public demand overwhelms the system."[23] Tragically, as Katrina reminds us, disasters can destroy all available terrestrial systems, meaning that the only way to assure reliability and available access is to incorporate a satellite component. In short, through some combination of public or commercial wireless and satellite systems, it is clear that public safety agencies need access to a system that will remain operational and available during emergencies and that will afford them with priority access.

---

[18] Mary Greczyn, *FCC Weighs Whether To Scrap 20-Year-Old Cellular Mandates*, COMMUNICATIONS DAILY (August 7, 2002) (reporting that digital cellular networks reached only around 50% of the population).

[19] James Careless, *Speak Easy: Technologies To Improve Two-Way Communications for First Responders*, FRONTLINE FIRST RESPONDER (June 2003) (http://www.msvlp.com/pr/pdf/speakeasyarticle.pdf).

[20] *Increasing FDNY's Preparedness*, August 19, 2002 (www.nyc.gov/html/fdny/html/mck_report/toc.html).

[21] Public Safety Wireless Network Program, *Public Safety In-Building/In-Tunnel Ordinances and Their Benefits to Interoperability Report* (November 2002) (http://www.safecomprogram.gov/NR/rdonlyres/2311FAAD-18DE-4EA9-BC5A-6C99CC24BAFA/0/In_Building_In_Tunnel_Ordinances_Report.pdf).

[22] United States House of Representatives, *A Failure of Initiative*, *supra* note 13, at 167.

[23] National Task Force on Interoperability, *When They Can't Talk, Lives Are Lost* (February 2003) (http://www.agileprogram.org/ntfi/ntfi_brochure.pdf).

C. *Interoperability*

As numerous policy observers and policymakers have emphasized, the lack of interoperability among public safety agencies remains a grave concern.[24] As the FCC has defined the issue, interoperability is "[a]n essential communications link within public safety and public service wireless communications systems which permits units from two or more different entities to interact with one another and to exchange information according to a prescribed method in order to achieve predictable results."[25] Stated more simply, interoperability means that two (or more) emergency service providers—say, a paramedic and a fire fighter—can communicate with one another in an efficient, reliable, and secure fashion. Going forward, however, interoperability needs to include more than "first responders 'talking to each other'; it needs to include inter-organizational data communications."[26] Accordingly, an understanding of *effective* communications should include the ability to exchange voice and data seamlessly.[27] Furthermore, interoperability should include the ability to access real time video feeds.[28]

Given the American system of government, with thousands of local agencies that enjoy local autonomy, it is not surprising that different jurisdictions (as well as, unfortunately, agencies within the same jurisdiction) have often made decisions that inadvertently do not promote interoperability. However, despite awareness of interoperability shortcomings and the expenditure of considerable funds, state and local governments "responsible for designing and coordinating their efforts" have largely "failed to make meaningful progress."[29] In view of this failure, the federal government is best positioned to help engineer such progress going forward. One commentator has rightly noted, it "is obvious that without effective coordination mechanisms, any communications infrastructure designed by many thousands of independent decision-makers is prone to producing a tangle of systems that do not interoperate."[30]

In looking back at the numerous inquiries into the causes of the continuing lack of interoperability, several themes emerge as predominant. First, many jurisdictions claim that they lack the funds to upgrade their systems (that are often 20-40 years old) and, more fundamentally, are unable to plan effectively for their wireless communications needs.[31] Second, local public safety administrators (either managers like the Chief of Police or the relevant IT professional working in an agency) are often attached to their current approaches and unwilling to give up control to facilitate a greater sharing of resources and technology. In this respect, achieving interoperability is not simply a matter of upgrading equipment, but also of changing the culture of operating in isolation and without full regard for how other public safety agencies operate.[32]

To be sure, there are some notable successful ventures that have galvanized regional cooperation between different agencies. Consider, for example, the Capital Wireless Integrated Network (CapWIN) project, which brings together over 40 local, state, and federal public safety agencies in the Washington, D.C. metro area into a system that provides important real-time communication abilities and access to government databases.[33] Such projects, however, require a system of effective governance involving a number of discrete agencies willing to coordinate their radio equipment needs. Notably, as many other failed initiatives demonstrate, ambitious visions of developing a single system to be used by all relevant agencies

---

[24] *See, e.g.*, Government Accountability Office, Protecting Structures and Improving Communications During Wildland Fires 24 (April 2005) (http://www.gao.gov/new.items/d05380.pdf) ("The lack of communications interoperability among firefighting and other first-responder agencies can impair their ability to respond to emergencies quickly and safely, and cost lives among responders and those they are trying to assist.").

[25] *The Development of Operational, Technical, and Spectrum Requirements For Meeting Federal, State, and Local Public Safety Agency Communication Requirements Through the Year 2010*, First Report and Order, 14 FCC Rcd 152 ¶ 76 (1998).

[26] National Reliability and Interoperability Council, Focus Group 1D, *Communications Issues Beyond E911* (December 2005).

[27] This idea is reflected in a recent definition of interoperability articulated by the House Bipartisan Committee: "the ability to share information via voice, data, on demand, in real-time, when needed and as authorized." United States House of Representatives, *A Failure of Initiative*, *supra* note 13, at 174.

[28] For example, the Wireless Accelerated Responder Network (WARN) project is a broadband safety network which permits interoperable, city-wide, real time video tools for remote surveillance and detection. Testimony of John M.R. Kneuer, Acting Assistant Secretary for Communications and Information, before the *Committee on Homeland Security's Subcommittee on Emergency Preparedness*, U.S. House of Representatives (April 25, 2006)(http://www.ntia.doc.gov/ntiahome/congress/2006/Kneuer_interoperable_042506.htm).

[29] *See* United States House of Representatives, *A Failure of Initiative*, *supra* note 13, at 174. To be sure, a number of states— such as Maryland, Nevada and Iowa— have launched public safety communications initiatives while others have worked cooperatively with other states through entities such as the National Governors Association Policy Academy on Wireless Interoperability. *See* NASCIO, *We Need to Talk: Governance Models to Advance Communications Interoperability*, 2-3 (November 2005) (http://www.nascio.org/nascioCommittees/interoperability/Interop.%20Gov.%20Research%20Brief%20Final.pdf).

[30] John Peha, *How America's Fragmented Approach to Public Safety Wastes Money and Spectrum*, *supra* note 15, at 2, 15. Moreover, Peha rightly notes that interoperability alone is not a panacea to be achieved without attention to other goals (such as cost-effectiveness and an architecture that will facilitate innovation) going forward.

[31] To help remedy this, the National Telecommunications and Information Administration has taken steps toward awarding $1 billion in grants that will emphasize public safety interoperability. *See* NTIA Making Progress In Planning for New Interoperability, DTV Programs, TR Daily (April 7, 2006).

[32] *See, e.g.,* National Reliability and Interoperability Council, Focus Group 1D, *Communications Issues Beyond E911* (December 2005) (advocating a conceptual shift so that "all emergency agencies, both public and private, [are viewed] as an overall 'enterprise,' rather than . . . isolated 'silos' that exist today."); *see also* "Are we there yet?" *Mobile Radio Technology* (December 1, 2005) (http://www.keepmedia.com/pubs/MobileRadioTechnology/2005/12/01/1116833) (A "silo approach to communication could become extinct . . . [as] it makes little fiscal sense to build a separate network for each department, when the government entity can build a universal network that serves all departments cost effectively.").

[33] *See generally* National Task Force on Interoperability, *Why Can't We Talk? Working Together to Bridge the Communications Gap to Save Lives—A Guide for Public Officials* 20 (February 2003) (http://www.safecomprogram.gov/NR/rdonlyres/322B4367-265C-45FB-8EEA-BD0FEBDA95A8/0/Why_cant_we_talk_NTFI_Guide.pdf).

are very difficult to achieve and thus more flexible approaches are far more likely to be successful.[34]

A third major cause of limited interoperability is that many agencies cannot communicate with one another because they use equipment with incompatible (and sometimes proprietary) technology. In some cases, these sorts of challenges can be addressed by developing intermediary patches—i.e., a dispatch center (using "bridge equipment") that can interconnect different systems—but such "second best" solutions are expensive and inefficient compared to more rationally designed systems.[35]

Although none have taken hold completely, there are a number of efforts that have attempted to overcome the lack of common standards and to develop ones to facilitate interoperable public safety communications. Notably, the APCO-sponsored Project 25 standard and the European-developed TETRA standard have both sought to advance this goal; more recently, the international "Project MESA" initiative has begun to develop a next generation standard.[36] In its effort to facilitate interoperability, the FCC chartered an advisory committee (the Public Safety National Coordination Committee) that has recommended technical and operational standards for spectrum that will be made available to public safety agencies.[37] Additionally, NTIA has spearheaded laudable standards-setting initiatives for public safety communications in conjunction with other agencies and programs.[38] Finally, the Department of Homeland Security's SAFECOM initiative has developed a "statement of requirements" that, in the words of SAFECOM's Director, provide an "architectural framework for future interoperable public safety communications."[39]

The final cause of limited interoperability is that local public safety agencies often lack access to radio spectrum in the same frequency bands used by sister agencies. As a result, public safety agencies—which use any one of ten different bands of spectrum—often cannot communicate with one another even when using compatible technology.[40] To rectify this situation, many in the public safety community have suggested that the transition to digital television, which will open up 24 MHz of spectrum in the valuable 700 MHz band for public safety uses,[41] should alleviate such concerns. But, to understate matters, it remains open to debate whether the transition will be completed by 2009.[42] Moreover, "no public safety agency can logically budget for equipment that uses radio spectrum that is not yet available for them."[43]

In evaluating the spectrum issue, it is important to make clear that this aspect of interoperability might be unsolvable because different agencies often have good reasons for choosing different bands. In short, there are big differences in propagation characteristics between the lowest frequency band and the higher frequency bands used by public safety agencies; consequently, agencies in, say, mountainous areas have compelling reasons for choosing different bands than those agencies in topologically different (and possibly adjacent) areas. Thus, even if the FCC could identify adequate available capacity, it would still be unwise to force all public safety agencies into a single band.

In light of the various forces that make interoperability at the physical layer difficult to achieve, it is critical that next generation systems not focus solely on this goal. In particular, new technologies can enable public safety radios to interoperate with one another at higher layers by using standard technologies (such as Internet Protocol) and specialized applications.[44] Such solutions are particularly attractive in the near

[34] National Task Force on Interoperability, *Why Can't We Talk: Working Together to Bridge The Communications Gap to Save Lives, Supplemental Resources* 19-22 (February 2003) (http://www.agileprogram.org/ntfi/ntfi_supplemental.pdf) (detailing Colorado's failed approach).

[35] For an excellent discussion of the spectral inefficiencies engendered by interoperability patches, *see* John Peha, *How America's Fragmented Approach to Public Safety Wastes Money and Spectrum*, *supra* note 15, at 6-10.

[36] More generally, certain equipment makers recently announced that they have formed the Communications Platforms Trade Association, which describes itself as "dedicated to accelerating the adoption of SIG-governed, open specification-based communications platforms through interoperability testing and certification." *See* CPTA Vision Statement, available at http://www.cpta.org/about/ (last checked April 26, 2006). To the extent such efforts are successful, these interoperability efforts represent another reason that public safety administrators should consider taking advantage of commercial systems.

[37] *See The Development of Operational, Technical, and Spectrum Requirements For Meeting Federal, State, and Local Public Safety Agency Communication Requirements Through the Year 2010*, WT Docket 96-86, Fifth Memorandum Opinion and Order, 20 FCC Rcd 831 (2005) (considering recommendations).

[38] NTIA is working with other agencies including the National Institute of Standards and Technology's Office of Law Enforcement Standards, DHS's SAFECOM Program, Department of Justice's Office of Community Oriented Policing Services, the Federal Partnership for Interoperable Communications, and DHS Chief Information Officer's Wireless Management Office. Collectively, these entities are trying to develop "a long-term standardized approach for nationwide communications interoperability and information sharing among local, State, and Federal public safety agencies, and short-term interim solutions to facilitate communications while the long-term approach is being completed." Testimony of John M.R. Kneuer, *supra* note 28.

[39] Press Release, *Homeland Security First to Define Interoperability Requirements for Nation's First Responder Community* (April 26, 2004) (http://www.dhs.gov/dhspublic/display?content=3513).

[40] A list of public safety spectrum allocations—97 MHz in total—is available in the *FCC Report to Congress, supra* note 2, at ¶ 5.

[41] *The Development of Operational, Technical, and Spectrum Requirements For Meeting Federal, State, and Local Public Safety Agency Communication Requirements Through the Year 2010*, First Report and Order, 14 FCC Rcd 152 (1998); *Reallocation of Television Channels 60-69, the 746-806 MHz Band*, Report and Order, 12 FCC Rcd 22,953 (1997); Balanced Budget Act of 1997, Pub. L. No. 105-33, § 3004, 111 Stat. 251 (1997) (codified at 47 U.S.C. § 337(a)(1)).

[42] *See* Jeffrey Silva, RCR Wireless News, *Controversial 700 MHz Plan Aims to Solve Public Safety Crisis: But DTV auction would be scrapped* (March 31, 2006) (https://www.rcrnews.com/lockland.cms?articleId=50338). For a perspective on how the DTV transition could be used to improve public safety, *see* Jon M. Peha, *The Digital TV Transition: A Chance to Enhance Public Safety and Improve Spectrum Auctions* (forthcoming in IEEE Communications) (http://www.ece.cmu.edu/~peha/DTV.pdf).

[43] *Why Can't We Talk*, *supra* note 33, at 53.

[44] The National Reliability and Interoperability Council, for example, suggests that integration can best be achieved through a "single, interconnected Internet Protocol system" for all emergency communications. *See* National Reliability

term insofar as they address existing challenges without requiring the immediate wholesale replacement of existing equipment. In a recent Report to Congress, the FCC noted that "IP-based systems are capable of enabling communications between diverse radio systems and frequencies without requiring the replacement of existing radios."[45] To promote just this sort of architecture, a coalition of first responders is now working to develop an Extensible Markup Language (XML)-based standard (i.e., the Emergency Data Exchange Language (EDXL)) to enable the panoply of different agencies that might be called to the scene of an accident (i.e., public safety, transportation, and medical personnel) to share information with one another.[46] Over time, efforts such as this one are likely to become critical parts of a next generation public safety communications system.[47]

D. Configurability and Flexibility

The ability of public safety networks to provide one-to-many communications (think "calling all cars") is essential to their effectiveness. Moreover, it is important that such networks be flexible and configurable so that they can include other groups (say, utilities when damage to an electric grid is involved) on an as-needed basis. In some cases, both of these features—i.e., a one-to-many functionality and an ability to create ad hoc networks of users—were lacking in traditional commercial networks. Increasingly, however, modern commercial networks (which are often software-based and designed for multiple applications) can support applications specialized for first responders, including sophisticated push-to-talk features. Additionally, configurability will be enhanced by the development of software defined networks where "functionality is built into the components at the factory, by allowing changes in parameters to be downloaded remotely."[48] In combination with smart antennae, mesh networks and cognitive radio, software defined networks promise to help tackle interoperability problems and make more efficient use of spectrum.[49]

E. Security

For public safety agencies, protecting the privacy of communications and guarding against malicious attacks on their communications services are critical priorities. To keep information private and guard against attacks, secure communications systems must encrypt communications (so that unauthorized users are not able to intercept them) and bilaterally authenticate both remote users and servers (to limit who has access to the system). In an ideal system, encryption keys can be dynamically assigned from a central management system so that additional users can be added as needed. Again, traditional commercial networks tend to lack sophisticated encryption and authentication capabilities. While security vulnerabilities have helped rationalize separate networks (which separation in turn has exacerbated interoperability problems), next generation solutions to security concerns and limited access to information resources "should be governed by cryptograph-ensured access control, not separate physical networks."[50] In this vein, next generation commercial systems will increasingly deploy more sophisticated security features—such as Public Key Infrastructure (PKI)—and allow for applications that can provide additional security (e.g., through the use of stronger encryption, such as NSA Type-1).

IV. A Hybrid Approach Incorporating LMR, Terrestrial, Emerging Wireless Broadband, and Satellite Services Will Provide Important Benefits to Public Safety Agencies

In evaluating the communication needs of public safety agencies, policymakers should reject the calls for a "one-size fits all" solution and recognize, as the Federal Wireless Policy Committee has put it, that "more than one service may be required to support" a next generation public safety network.[51] Furthermore, as one commentator has prescribed, "federal policy makers must resist the temptation to impose 'apartheid', treating public safety networks as so special that they must be quarantined on frequencies of their own. Emergency radio services need to exit their government technology ghetto and get onboard advanced networks—as smart customers, not Soviet-style suppliers."[52] In particular, policymakers should promote a hybrid approach that would incorporate LMR systems along with traditional terrestrial, satellite, and emerging wireless broadband systems.

---

and Interoperability Council, Focus Group 1D, *Communications Issues Beyond E911* (December 2005).

[45] *FCC Report to Congress* dated December, 19, 2005, *supra* note 2, at ¶ 47

[46] Diane Frank, *First Responders Seek Common Lingo*, FEDERAL COMPUTER WEEK (March 15, 2004) (http://www.fcw.com/article84556).

[47] For an example of one vendor's proposed IP-based interoperability solution, *see* Cisco Systems White Paper, *Solutions for Communications Interoperability* 2-3 (2005) (http://www.cisco.com/en/US/products/ps6718/products_white_paper0900aecd80350fee.shtml) (opining that "IP networking provides the most viable solution to communications interoperability. It is critical that any selected interoperability solution is flexible and modular to incorporate new technologies as well as guarantee investment protection.").

[48] Moore, *supra* note 1, at 15-16. For additional detail concerning software defined radios, *see, e.g.,* International Telecommunication Union, Radiocommunication Study Groups, Working Party 8F, *The Impact of Software Defined Radio on IMT-2000, The Future Development of IMT-2000 and Systems Beyond IMT-2000*, Document 8/89-E (August 2005).

[49] *Id.*

[50] *See* National Reliability and Interoperability Council, Focus Group 1D, *Communications Issues Beyond E911* (December 2005).

[51] Federal Wireless Policy Committee, *Federal Functional Requirements for Commercial Wireless Services* (Dec. 11, 2001) (http://www.fwuf.gov/docs/rev_dec01.pdf); *see also* James Careless, *Speak Easy: Technologies To Improve Two-Way Communications for First Responders*, FRONTLINE FIRST RESPONDER (June 2003) (http://www.msvlp.com/pr/pdf/speakeasyarticle.pdf) (highlighting virtues of a multi-mode solution); Michael McShea & Richard Davis, *A Hybrid Approach*, MISSION CRITICAL COMMUNICATIONS 57 (April 2005); Alan Shark, *Don't Rule Out Either Option*, MISSION CRITICAL COMMUNICATIONS 60 (April 2005) ("no one system can or should meet all jurisdictional mission-critical needs").

[52] Thomas Hazlett, *Katrina's Radio Silence*, Financial Times (October 26, 2005).

Solutions premised on a flexible architecture are only beginning to be tested, but it is increasingly apparent that traditional LMR systems can be provided along with ancillary terrestrial component satellite handsets that automatically switch between cellular and satellite systems (depending on which is available). Moreover, by designing such systems in a modular fashion, they can rely on wireless broadband networks, such as those using WiFi technology as well as still emerging technologies (like the next generation WiMAX standard). Notably, a WiFi-like system, like satellite technology itself, is relatively robust and, as demonstrated in the aftermath of Katrina, can be important in assisting the communications needs of public safety agencies.[53] Significantly, a hybrid approach allows leaders in public safety communications to leverage current innovations in wireless broadband in combination with other technologies.

One important reason for relying on commercial systems in general and hybrid satellite-terrestrial systems in particular is that they enable public safety agencies to benefit from the considerable economies of scale and enhanced functionalities that commercial providers can offer. Even under the very best of circumstances, public safety agencies are generally not able to build up the economies of scale and develop the network efficiencies of their commercial brethren. (This explains, in considerable part, why public safety equipment is generally quite expensive.) At a minimum, then, public safety agencies should take advantage of the favorable economics of commercial systems and "off the shelf" equipment for at least some of their communications needs.[54] As we explain below, satellite services in general and hybrid satellite-terrestrial offerings in particular meet the requirements outlined above and are well suited to be a valuable component of public safety wireless systems.

To supplement traditional terrestrial networks, it is critical to incorporate satellite services into public safety wireless systems.[55] First, as Katrina made clear, satellite systems are the best means of ensuring that public safety communication systems remain operational during dire circumstances. Second, satellite technology can assure complete coverage to public safety agencies. For example, the New Mexico State Police Department has compensated for the lack of ubiquitous coverage and ability to carry data on its private LMR by contracting with a satellite firm for access to a satellite-based solution that provides ubiquitous coverage, reliable push-to-talk services, and access to data communications capabilities.

Finally, with the approved ATC architecture that firms will begin rolling out for hybrid satellite-terrestrial systems, the price of satellite services are projected to be substantially less than current satellite systems (on account of its use of mainstream devices as well as more efficient terrestrial systems where appropriate). Notably, the price of this service will decline dramatically as subscribers adopt it and the network enjoys greater scale economies. Significantly, even as to one of the advertised strengths of private LMR systems *vis-à-vis* commercial networks—the ability to provide coverage wherever it is needed—hybrid satellite-terrestrial systems can provide the best of both the commercial model as well as the traditional LMR systems. Thus, for carriers looking at the expense of adopting new LMR systems for remote areas and the ongoing costs of maintaining the necessary equipment, a hybrid satellite-terrestrial system provides an exciting alternative.

Deployment of ATC services should allow satellite firms to provide attractive wireless communications products that are reliable and flexible. Unlike most commercial networks, hybrid satellite-terrestrial systems can be used when the local power grid fails or, in a situation like Katrina, when the available terrestrial networks are rendered inoperable. In particular, hybrid satellite-terrestrial handsets can switch seamlessly between cellular networks (when a base station is operating nearby) and a satellite network (when there are no base stations in the area). These systems can and should be designed so that, in the case of emergency events, the public safety operators enjoy priority access to the extent necessary to preserve public safety communications.

In terms of flexibility and configurability, hybrid satellite-terrestrial systems can be designed to allow for the creation of ad hoc user groups that can use push-to-talk functionality and communicate among an interdisciplinary team through a large group dispatch service. Significantly, the set-up time for such push-to-talk functionality is expected to be similar to existing satellite offerings (i.e., with a couple of seconds for call set-up and a short delay between speakers). To be sure, this system may not be appropriate for "shoot-don't-shoot" situations, but it will be entirely adequate for an array of scenarios where push-to-talk systems are used by public safety agencies, including nearly all of the first responder communications needs in the wake of Katrina.

Increasing their reliance on commercial systems such as hybrid satellite-terrestrial systems does not mean that public safety agencies should abandon their existing LMR systems. Rather, today's LMR systems often serve a very useful purpose and should be an important part of a hybrid network ar-

[53] Kenneth Moran, Presentation at the Agenda Meeting of the Federal Communications Commission (September 15, 2005); *see also* Clive Thompson, Talking In The Dark, N.Y. Times Magazine 24 (September 18, 2005) (discussing how Wi-Fi-like systems using mesh technology can provide reliance and redundant communication networks).

[54] For example, Iridium Satellite LLC recently announced satellite telephone communications equipment which is interoperable "with existing UHF and VHF radio systems already used by police, rescue agencies, firefighters and other first responders." The system costs about $10,000. Todd Weiss, Computerworld, *Iridium trumpets latest satellite phones for emergency response* (May 1, 2006) (http://www.computerworld.com/securitytopics/security/recovery/story/0,10801,111058,00.html?from=story_kc).

[55] As the FCC recently explained, satellite services "provide ubiquitous, reliable coverage throughout the United States and are generally immune from natural and manmade disasters. *FCC Report to Congress* dated December, 19, 2005, *supra* note 2, at .¶ 29.

chitecture. Along these very lines, both mission critical networks and critical infrastructure companies (such as utilities like the Tennessee Valley Authority) have begun to gravitate away from relying solely on their private networks. In particular, a number of entities that previously relied solely on their LMRs have concluded that they should continue to maintain such networks, but rather than upgrade them, they can increase productivity and cut costs by moving towards an integrated architecture that includes commercial wireless networks.

In terms of developing an optimal network architecture, public safety agencies should also be open to taking advantage of advances in wireless broadband technology developed for unlicensed spectrum.[56] A public safety network might use, for example, current wireless local area network (WLAN) technology (i.e., the 802.11 (WiFi) standard) and, eventually, next generation systems (e.g., 802.16 (WiMAX) systems). To foster the adoption of such systems by local governments, the FCC recently made available access to spectrum in the 4.9 GHz band. As the FCC stated in its press release, "public safety licensees [can now] use a single, low-cost device to access the 4.9 GHz band, the U-NII band, and the ITS band, allowing them to enjoy savings that are typically limited to the high-volume commercial market."[57] Recognizing this opportunity, some police departments, like that of Salida, Colorado, have adopted solutions based on this technology, saving money and making police officers more productive in the process.[58]

One means of providing wireless broadband service is to use ad hoc mesh networking systems. At present, such systems are still in their early stages.[59] Such systems promise (as one vendor put it) "infrastructure-free, automatically established and maintained, and agile" network architectures.[60] The promised effectiveness of such systems, which rely on a different architecture from today's established wireless technologies, reflects their ability to "forward data one hop at a time over a distributed network of autonomous nodes using new and more reliable and efficient schemes."[61] To limit the need for a widespread deployment of devices with the embedded ability to re-transmit communications (i.e., routers), some cities have deployed systems with transmitters placed on existing infrastructure (like streetlamps) and with intelligent access points to connect to wired infrastructure at particular points. In Garland, Texas, for example, the local law enforcement agency decided to rely on such a network, concluding (after an experimental use of the technology on a limited basis) that installing access points and wireless routers on existing infrastructure would be cheaper than building new transmission towers for either cellular or private LMR transmissions towers.[62] Finally, mesh networking systems, which rely on the basic Internet suite of protocols, can be secured by installing firewalls and other security protections.

In short, an optimal public safety architecture would use a flexible system to accommodate different technologies. As depicted in Figure 1 below, a public safety agency can use a multi-mode device to access a hierarchy of wireless networks, beginning with a public safety LMR system at the center, then a commercial terrestrial network such as an ATC service and finally a satellite overlay.[63] As noted above, public safety agencies might also choose to integrate a terrestrial wireless broadband network. In any event, the core design principle is that networks should be extensible to other terrestrial networks in addition to the core commercial terrestrial and satellite components.[64]

Both commercial and public safety-driven considerations explain why multi-mode networks are increasingly practical and appropriate. Consider, for example, that today's ordinary consumer wireless devices have two to four bands and at least some of tomorrow's devices will use WiFi networks where available. With an extensible network, the keys to integrating them together are (1) facilitating the back-end integration of the commercial network and one or more LMR systems; and (2) gradually adding new user devices that incorporate satellite connectivity, including push-to-talk. In principle, this integration can be accomplished by incorporating a second chipset that would enable the device to use a satellite-adapted version

[56] For a summary of examples of "Public Safety Deployments on Unlicensed Airwaves" in 14 different cities and towns in the United States, *see* Naveen Lakshmipathy, *Wireless Public Safety Data Networks Operating on Unlicensed Airwaves: Overview and Profiles*, New America Foundation, 4-8 (Updated April 12, 2006) (http://www.newamerica.net/Download_Docs/pdfs/Doc_File_2633_1.pdf).

[57] News Release, FCC Improves Public Safety Access To The Latest Broadband Technology (November 9, 2004) (http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-254117A1.doc).

[58] Jim Renton, *Notebooks and Wi-fi Keep Colorado Cops on the Beat*, MOBILE COMPUTING NEWS (March 8, 2004) (http://searchmobilecomputing.techtarget.com/originalContent/0,289142,sid40_gci953936,00.html?track= NL-315&ad=477866&Offer=t3.8); *see also Metro-Scale Wi-Fi for Public Safety: San Mateo Police Department*, A Tropos Networks Case Study (March 2004) (summarizing San Mateo police department's use of Wi-Fi-based wireless broadband).

[59] As of June 2005, Medford, Oregon, San Mateo, California, North Miami Beach, Florida, and Garland, Texas had undertaken efforts to use mesh networks for public safety. *See* Moore, *supra* note 1, at 16.

[60] Michael Rauf & Eric Lefebvre, *Keeping the Wireless Connection Running*, 9-1-1 MAGAZINE 58 (Jan/Feb 2003) (http://www.novaroam.com/downloads/nr_911article.pdf)

[61] Rick Merritt, *Darpa Looks Past Ethernet, IP Nets*, EE TIMES (April 26, 2004) (http://www.eet.com/showArticle.jhtml?articleID=19200111).

[62] Kris Middaugh, *No More Towers*, GOVERNMENT TECHNOLOGY (May 2004) (http://www.govtech.net/magazine/story.php?id=90189).

[63] Hybrid satellite-terrestrial systems rely on a satellite system that uses the same band of spectrum for an integrated terrestrial system. With such a system, important spectrum efficiencies and economies of scale will be achieved which will result in lower cost and more user-friendly consumer equipment than current MSS equipment. Such advancements are critical to deployment of next generation systems and will redound to the benefit of public safety agencies that adopt it.

[64] For a different conceptual framework in the way of a "Future Internetwork Architecture," *see* National Reliability and Interoperability Council, Focus Group 1D, *Communications Issues Beyond E911* (December 2005) (setting forth an network architectural scheme premised on the belief that "effective future emergency communications systems need to be linked in an 'internetwork' – a set of policies, tools, interfaces and standards that connect securely the multiplicity of local, regional and national wireline and wireless networks.")

of a mass-market air interface (MMI) such as GPRS, CDMA, OFDM or WiMAX.

Although the cost of a module with the chipset necessary to enable a hybrid terrestrial-satellite system is likely to be more than the additional cost of the consumer ATC product, it will almost certainly be substantially less than equipment developed only for public safety agencies (i.e., on account of the economies of scale resulting from the consumer deployment of ATC). Notably, embracing a flexible, hybrid architecture will almost certainly be cheaper than investing in the software and equipment necessary to achieve interoperability solely by upgrading or replacing existing LMRs.[65] Moreover, achieving interoperability through a flexible architecture (i.e, one that can facilitate ad hoc user groups through shared terrestrial and satellite systems) can be done relatively quickly and cheaply (at least when compared with SAFECOM's projection for achieving interoperability along the current path[66]) and would also provide critical redundancy benefits.

Ultimately, the network depicted in Figure 1 below would include an overlay for public safety purposes. Significantly, the concept of such a virtual network could be implemented using the same capabilities that mobile virtual network operators (VNO)[67] use today. In order to ensure control, security, and availability, the core network would dedicate resources to the Public Safety VNO, which would operate the public safety serving-network based on applications and policies of its own choosing. The public safety agency would also have the option not only to integrate a multi-mode radio using physically separate modules, but ultimately to use software-defined radios to switch seamlessly between different networks and their associated functionalities.[68]

The vision of using "smart radios" for public safety communications systems would, as Chairman Martin put it, enable them to use "multiple frequencies in multiple formats" and would facilitate a more "flexible infrastructure."[69] Notably, while the United States' Department of Defense is a leader in the development of software defined radio technologies, smart radio research and concomitant efforts to assimilate such innovations into public safety communications are international in scope.[70] Such efforts promise to "enable operability among public safety agencies on multiple air interfaces, overlaying existing systems without disruption, upgrading legacy systems, including possible transition from one radio interface to another, and the easy selection of RF band, air interface, and group affiliation by users of portable SDR equipment."[71]

As part of such a flexible infrastructure, Chairman Martin has emphasized that public safety agencies would incorporate the use of satellite networks because they "are, in some instances, the most effective means of communicating."[72] Consequently, by using devices like that depicted in Figure 2, public safety agencies could benefit by using a combination of different networks and thereby enjoy (as Figure 1 reflects) a far more impressive footprint and greater level of redundancy than any individual system could offer on its own. Indeed, many public safety agencies recognize the need to incorporate multiple technologies into their system, but are looking for the leadership on what architecture to use as well as financial assistance to upgrade their systems.[73]

---

[65] Chief Willis Carter, Statement to Senate Commerce Committee 9 (September 29, 2005) (http://commerce.senate.gov/pdf/chiefcarter.pdf) (estimating that improving existing radios to allow interoperability would cost $800 per radio).

[66] The long term vision of SAFECOM foresees achieving interoperability by 2023. *See* David Boyd, Statement to the Senate Commerce Committee, Session on Communications Interoperability 2 (September 29, 2005) (http://commerce.senate.gov/pdf/boyd.pdf).

[67] Mobile Virtual Network Operators (MVNOs) lack network infrastructure or licensed spectrum, but instead use another operator's facilities and capacity to provide an alternative service. In a number of cases, they also possess the back-end systems and enhanced functionalities necessary to provide their service.

[68] *See generally FCC Report to Congress* dated December, 19, 2005, *supra* note 2, at ¶¶ 27, 47.

[69] September 22, 2005 Statement of Kevin J. Martin, *supra* note 6, at 7. Chairman Martin's observation echoed the findings of an earlier GAO Report. That report explained that "[s]oftware-defined radios will allow interoperability among different agencies using different frequency bands, different operational modes (digital or analog), proprietary systems from different manufacturers, or different modulations (such as AM or FM)." Government Accountability Office, *Protecting Structures and Improving Communications During Wildland Fires*, *supra* note 24, at 61-62.

[70] International Telecommunication Union, Canada and New Zealand, *Proposal for the Work on Software Defined Radio Within Study Group 8*, Document 8/124-E, 19 (November 2005).

[71] *Id.*

[72] September 22, 2005 Statement of Kevin J. Martin, *supra* note 6.

[73] Chief Willis Carter, Statement to Senate Commerce Committee 9 (September 29, 2005) (http://commerce.senate.gov/pdf/chiefcarter.pdf) (explaining that satellite technology must be a part of a solution that incorporates multiple approaches).

Figure 1 (note: diagram is conceptual in nature and not drawn to scale)

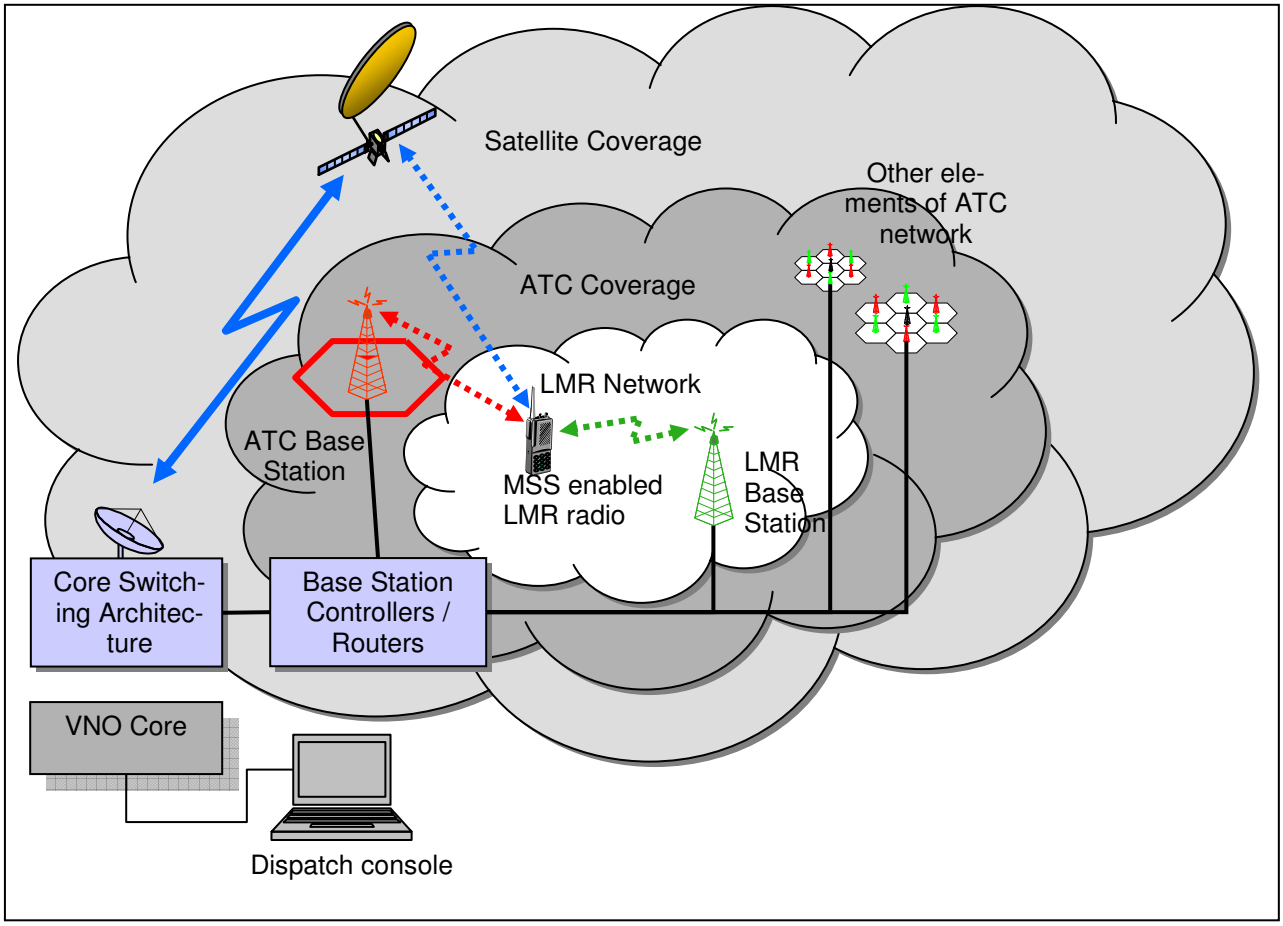
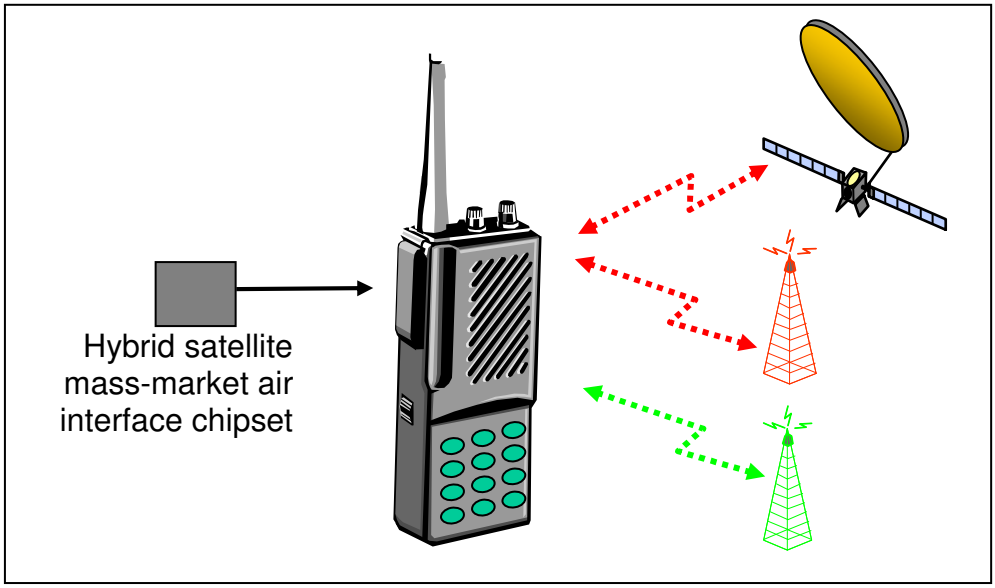


Figure 2 (note: diagram is conceptual in nature and not drawn to scale)



V. **A Policy Strategy For A Next Generation Public Safety Network**

The federal government can play a very important role in facilitating the development of an interoperable broadband mobile communications network for public safety agencies. The best strategy, as suggested above, is not necessarily to promote next generation private LMR systems operated by local public safety agencies. Indeed, committing to such a limited vision might well prove problematic on a number of scores (e.g., locking in a costly and potentially inferior technology). Rather, the government should appreciate that the ideal mix between public and commercial networks is one it cannot divine in advance and it should thus promote a hybrid model of public safety networks such as that outlined above. To implement such an approach, we recommend three critical regulatory strategies: (1) make additional spectrum available that can be used for public safety applications by commercial providers; (2) recognize that a policy of spectrum flexibility benefits public safety agencies by enabling commercial providers to meet their needs; and (3) ensure that additional appropriations to aid the development of public safety communications promotes the flexible architecture described herein.

A. Making More Spectrum Available for Public Safety Purposes

For quite some time, the discussion over "making available additional spectrum for public safety agencies" has focused on dedicating spectrum for private LMR systems operated by specific agencies. Moreover, this discussion has often centered on the 1996 recommendation by the Public Safety Wireless Advisory Committee that 25 MHz of spectrum was needed by 2001 for public safety purposes, with an additional 72.5 MHz required by 2010. Notably, this recommendation assumes both that (1) achieving interoperability and providing mobile broadband capability will require more spectrum to be specifically dedicated to public safety providers; and that (2) the transition to digital television will be completed in a timely manner so as to free up spectrum for this purpose. Both propositions, however, are far from clear, thereby raising the question of what alternative strategy policymakers might use to enable public safety agencies to migrate toward a next generation network.

Many policymakers continue to take the traditional perspective of focusing on particular spectrum as designated for certain purposes. In the case of public safety, the historical use of spectrum in and around the 700 MHz band makes it understandable that policymakers would focus on whether additional spectrum in this band is necessary to facilitate the transition toward a next generation public safety communications system. But policymakers should be careful not to indulge the two assumptions identified above—that providing specialized public safety spectrum is necessarily the best policy and that the digital transition will be completed in a manner that will make available such spectrum in a timely fashion. Rather than indulge such assumptions, we urge policymakers to think more broadly about what it means to make more spectrum available for public safety uses.

A broader perspective on the issue would appreciate that the Commission's recent action related to enabling public safety agencies to use spectrum in the 4.9 GHz band for wireless broadband is a form of making additional public safety spectrum available. Thinking even more broadly, it is clear that flexible policies related to Specialized Mobile Radio (SMR) spectrum—including its decision to allow Nextel (now Sprint/Nextel) to accumulate dispatch licenses—promoted the development of public safety spectrum, as many public safety agencies now use Nextel's services and benefit from its economies of scale. Similarly, the Commission's policies authorizing the use of ATC—as well as its efforts now underway to finalize the distribution of surrendered MSS spectrum in the S Band—promise to make available spectrum that will be commercialized in a manner that will benefit public safety agencies.[74]

In short, policymakers should appreciate the importance of committing spectrum to commercial providers capable of offering service to public safety agencies. In the case of satellite providers, it is not merely sufficient for the FCC to allocate spectrum for use by satellite providers, but it is also critical for it to provide certain and stable assignments of satellite spectrum. Only with such stable assignments, and the ability for providers to undertake significant investments over a period of time, will satellite providers be able to deploy innovative offerings like a hybrid satellite-terrestrial system that will ultimately benefit public safety agencies as well as other consumers.

B. A Policy of Spectrum Flexibility Benefits Public Safety Agencies

It is crucial that policymakers appreciate how promoting spectrum flexibility will greatly benefit public safety agencies. This approach is consistent with the FCC's stated recognition that "in order for public safety entities to successfully carry out their missions, they must rely on a forward-looking spectrum policy that promotes beneficial technological advances into their communications system."[75] Notably, the Spectrum Policy Task Force Working Group on Spectrum Rights and Responsibilities explained the innovation suffocating vices of the less than prescient old approach:

---

[74] The Commission expressly recognized the public safety benefits of ATC in authorizing its use, concluding that "ATC may enhance the nation's overall ability to maintain critical telecommunications infrastructure in times of crisis or disaster." *Flexibility for Delivery of Communications by Mobile Satellite Service Providers in the 2GHz Band, the L-Band, and the 1.6/2.4 GHz* Bands, Report and Order, 18 FCC Rcd 1962, ¶ 29 (February 10, 2003).

[75] Federal Communications Commission, Eighth Notice of Proposed Rulemaking, *In the Matter of The Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Communications Requirements Through the Year 2010* 13 (released March 21, 2006) (http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-06-34A1.pdf).

> From the Commission's experience with command-and-control regulation, it is apparent that overregulation can deter both efficiency and innovation. The highly regulated nature of certain services has tended to discourage technological change because the means of providing permissible services are narrowly defined in terms of current and outdated technology. Moreover, in cases where licensees are limited in what services they are permitted to offer, they have no incentive to seek out a higher valued use for the spectrum.[76]

The Commission's new perspective on spectrum policy takes a fairly critical perspective toward the classic "wise man" restrictions on how spectrum can be used and instead calls for "a light touch and a sense of humility" in developing rules that restrict uses of the spectrum.[77] Thus, as the FCC's Spectrum Policy Task Force concluded, the Commission should look "to increase opportunities for technologically innovative and economically efficient spectrum use, spectrum policy must evolve toward more flexible and market-oriented regulatory models."[78]

By reforming its traditional policy toward spectrum management, the Commission will, as Chairman Martin explained, move toward a model of "flexible allocations (that are technology and service-neutral)" of spectrum licenses.[79] This model, which the Commission has begun promoting through initiatives such as its Secondary Markets Order,[80] promises to "create strong incentives for making use of excess capacity" of spectrum already allocated in inflexible ways.[81] Significantly, by continuing to make progress on spectrum reform more generally, policymakers can assist public safety agencies in particular by helping to make the network architecture outlined above more effective and less expensive.

C. Funding For Public Safety Agencies Should Promote A Flexible Architecture

For many public safety agencies, their first priority and instinctive response is to replace their old equipment with expensive, proprietary, and single-use systems. In many respects, public safety agencies' attachment to LMRs of the kind that have served them relatively well is readily understandable—after all, familiarity often leads to comfort.[82] In the case of technology products like mobile radios, however, public safety agencies should appreciate that (1) multi-mode radios; (2) economies of scale from off-the-shelf and commercially provided products; and (3) the opportunity to incorporate satellite backup into their systems are all opportunities that are ignored only to the public's detriment. In providing important leadership on this issue, the federal and state governments should not allow local purchasing agents to act on auto-pilot and miss the option to migrate to a flexible, next generation architecture. Most important of all, policymakers should avoid requiring or creating incentives that would have the effect of foreclosing the type of architecture embraced by this article.

VI. CONCLUSION

To learn from what went right and wrong in the aftermath of Hurricane Katrina, policymakers should avoid the impulse to assume that simply granting more spectrum for public safety agencies and appropriating more money to invest in LMRs will solve the problems of public safety communications. Rather, both policymakers and the public safety agencies themselves should look beyond this traditional mindset and develop a next generation architecture that would incorporate satellite, terrestrial, and emerging wireless broadband networks into a single seamless system. To promote this system, policymakers should focus on making spectrum *generally* available for broadband uses, whether via unlicensed WiFi-like systems, licensed commercial carriers, or satellite providers (including those using hybrid satellite-terrestrial networks with the aid of ATC technology) and ensuring that any government funding promotes a flexible architecture for public safety communications. By so doing, policymakers can best advance a next generation public safety communications strategy that can provide a reliable, survivable, and secure network for all first responders.

Particularly in light of the lessons underscored by Hurricane Katrina, adhering to the traditional model of relying solely on LMRs is no longer sustainable and policymakers must consider a more flexible and robust next generation architecture for public safety communications. Significantly, such a system would facilitate the greater use of satellite technology, such as was used effectively in New Orleans and the Gulf Coast in the wake of Katrina, and would embrace the use of hybrid satellite-terrestrial systems. In so doing, policymakers

---

[76] Federal Communications Commission Spectrum Policy Task Force, *Report of the Spectrum Rights and Responsibilities Working Group* 11 (November 15, 2002) (http://www.fcc.gov/sptf/files/SRRWGFinalReport.pdf).

[77] Jonathan S. Adelstein, *New Frontiers in Wireless Policy: A Framework for Innovation* 3 (April 9, 2003) (http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-233139A1.pdf).

[78] Federal Communications Commission Spectrum Policy Task Force, *Spectrum Policy Task Force Report* 3, ET Docket No. 02-135 (November 15, 2002).

[79] Kevin J. Martin, *U.S. Spectrum Policy: Convergence or Co-Existence?* (March 5, 2002) (http://www.fcc.gov/Speeches/Martin/2002/spkjm202.html).

[80] *Promoting Efficient Use of Spectrum Through Elimination of Barriers to the Development of Secondary Markets*, Report and Order, 18 FCC Rcd 20,604 (2003).

[81] Kevin J. Martin, *U.S. Spectrum Policy: Convergence or Co-Existence?, supra* note 79.

[82] For example, consider the initial reluctance concerning radio-over-IP systems. When such systems emerged, "first responders wanted no part of them, fearing delay and connectivity problems associated with packet loss." *See* "Are we there yet?" *Mobile Radio Technology* (December 1, 2005) (http://www.keepmedia.com/pubs/MobileRadioTechnology/2005/12/01/1116833).

would make available far more cost-effective access to satellite technology than today's satellite terminals and ensure that users of this technology only utilize satellite capacity when it is truly needed. And most importantly, such networks would switch seamlessly between available networks to enable first responders to use a single handset and not worry about what network is optimal; instead, the device would automatically select the appropriate network.

By implementing effective spectrum policies, encouraging the development of hybrid solutions, and funding the purchase of more technically advanced solutions (e.g., multi-mode radios that include satellite and other technologies), policymakers can advance a next generation public safety network strategy. Notably, by promoting a public safety network where agencies can use spectrum licensed to commercial providers, available in unlicensed bands as well as dedicated to their private LMRs, public safety agencies will gain the benefits of a modern, innovation-rich, low cost network. In particular, public safety agencies will benefit from modular, extensible networks that can take advantage of cutting edge applications that ride on their private LMR, a commercially provided system, or an unlicensed wireless broadband network. If, by contrast, policymakers focus exclusively on supporting specialized equipment for LMRs and dedicated spectrum (say, in the 700 MHz band), they risk pursuing an antiquated technological architecture that will continue to leave public safety agencies without the best available tools for interoperable, reliable, secure, and broadband communications.[83]

[83] By proposing a radical departure from the current model, and in embracing an approach similar to the one advocated here, Nextel co-founder Morgan O'Brien is challenging the current policy trajectory and may well be able to focus the debate on what the appropriate model for a next generation architecture and how policymakers can implement it most effectively. *See* Petition for Rule Making, Reallocation of 30 MHz of 700 MHz Spectrum (747-762/777-792) From Commercial Use (April 27, 2006) (http://www.cyrencall.com/downloads/CyrenCall_FCC_Filing_060427.pdf).