ISSUES IN SCIENCE AND TECHNOLOGY
NATIONAL ACADEMY OF SCIENCES
ARIZONA STATE UNIVERSITY

VOL. XXIII, NO. 2, WINTER 2007

# Improving Public Safety Communications

BY JON M. PEHA

*Today's system puts the lives of first responders and the public at risk. What's needed is a nationwide broadband network, and policymakers now have a perfect opportunity to act.*

At 9:59 a.m. on September 11, 2001, the first of many evacuation orders was transmitted to police and firefighters in the World Trade Center's North Tower. Police heard the order, and most left safely. But firefighters could not receive the order on their communications equipment—even as people watching television at home knew of the tragedy unfolding. When the tower fell 29 minutes after the first evacuation order, 121 firefighters were still inside. None survived.

Although the number of lives lost on 9/11 was especially great, there is nothing unusual about loss of life due to failures in the communications systems used by first responders: firefighters, police, paramedics, and members of the National Guard. Such failures occur across the country during large disasters, such as Hurricane Katrina, and during emergencies

too small to make the news, such as police car chases and burning houses. When public safety communications systems do not work, the lives of first responders and the citizens they protect are at risk.

Clearly, the nation's public safety communications system is broken, and fundamental changes in technology and public policy are needed. Incremental changes here and there will not suffice. The weaknesses of the current system can be addressed only by developing a nationwide broadband communications network designed as an integrated infrastructure. Fortunately, the resources for such a move are now available; we need only the vision to use them well. In 2009, as part of the transition to digital television, the federal government plans to transfer a large portion of premium spectrum—24 megahertz (MHz)—from analog TV to public safety use. A block of this size, unencumbered with old equipment, is an extraordinary opportunity. Moreover, this segment of spectrum is around 700 MHz, which means it has physical properties that are particularly useful when designing a communications system that must cover a large geographic region, as would be required to adequately serve all first responders. But unless policymakers make concerted efforts to capitalize on the expanded spectrum for public safety, this rich opportunity will be lost.

In a strangely unrelated effort, the federal government also has plans to invest $3 billion to $30 billion and a significant amount of spectrum in the Integrated Wireless Network (IWN) program, which is intended to provide communications services for a tiny fraction of first responders. These resources could instead be used to serve all first responders.

## PROSPECTS FOR CRITICAL PROGRESS

Public policies on communications systems for public safety have evolved over many decades, and most of them have long outlived their usefulness. In particular, these polices are based on assumptions that local agencies should have maximal flexibility at the expense of standardization and regional planning, that commercial carriers have little role to play, that public safety should not share spectrum or infrastructure, and that narrowband voice applications should dominate. These policies have led to a system that fails too often, costs too much, consumes too much spectrum, and provides too few capabilities. Moreover, public safety requirements have changed after 9/11, and the technology has changed as well, so there are many reasons to consider a fundamental change in policy.

Public safety communications systems will remain inadequate as long as primary responsibility rests with local governments. Tens of thousands of independent uncoordinated agencies simply cannot design and operate a public safety communications infrastructure that meets the country's post-9/11 needs. Public safety officials must start planning over large geographic regions and large blocks of spectrum, and this requires fundamental reform. Policy

reforms should include shifting some responsibility and authority for decisions about public safety communications infrastructure from many independent local government agencies to the federal government, expanding the role of commercial service providers, allowing public safety to share spectrum with others, and expanding capabilities beyond traditional voice communications. Since the TV band spectrum to be reallocated to public safety has few legacy systems that must be accommodated or moved, it is an excellent place to launch a new policy.

Taking a new approach to public safety communications holds promise of making progress in a number of critical areas:

---

*PUBLIC SAFETY COMMUNICATIONS SYSTEMS WILL REMAIN INADEQUATE AS LONG AS PRIMARY RESPONSIBILITY RESTS WITH LOCAL GOVERNMENTS.*

---

*Interoperability*. Interoperability is the ability of individuals from different organizations to communicate and share information. Its lack is often cited as a major problem for public safety. For example, when first responders from multiple public safety agencies arrived at Columbine High School after the shooting in 1999, interoperability problems were so great that the responders had to rely on runners to carry written messages from one agency's command center to another. Interoperability is a problem only because decisions are made by local agencies, each of which has the flexibility to choose technology that is incompatible with that of its neighbors.

*Spectral efficiency*. Many public safety agencies have expressed concern that a shortage of public safety spectrum is coming, even assuming they do get 24 MHz of television spectrum. This shortage may have more to do with ineffective policy than technical necessity, because much greater efficiency is possible. If public safety systems have a spectrum shortage, their communications capacity will be inadequate during large emergencies. If the nation responds to the shortage by simply allocating more spectrum to public safety without improving efficiency, this wasted spectrum will be unavailable for other purposes such as inexpensive Internet access and cellular phone services.

*Dependability and fault tolerance*. Critical pieces of the system should rarely fail. Of course, some failures are inevitable when a hurricane the size of Katrina hits, but this need not bring down an entire system. In a fault-tolerant design, other parts of the system will continue to operate, compensating for failures to the extent possible. This can occur only if systems are designed coherently across large regions. Moreover, today's policies make it difficult for first

responders to use commercial systems, even when these are the only systems that survive a disaster such as a hurricane.

*Advanced capabilities*. Current public safety communications systems primarily provide voice. There are many other services that could be useful, including broadband data transfers, real-time video, and geolocation, which would enable dispatchers to track the precise location of first responders during an emergency.

*Security*. Systems can be designed so that hostile parties cannot easily attack a system or eavesdrop on first responders. The greatest challenge will be in protecting interagency communications, because protection must run "end to end," and today the agencies at each end of the conversation often have dissimilar technologies.

*Cost*. The uncoordinated actions of local agencies greatly increase costs. The amount of infrastructure deployed in a region today depends more on the number of local governments involved than on the region's size or population. Moreover, the rapid growth of commercial wireless services has led to mass production and low costs. Thus, equipment used by public safety could be much cheaper than was once possible, if it is similar enough to equipment used in commercial markets.

Recent efforts at reform have tended to address one problem at a time, which can make matters even worse. For example, the government has reallocated spectrum to address spectrum scarcity, but in a manner that may lead to new interoperability problems. There are grant programs specifically intended to improve interoperability, but some grants will be spent in ways that improve interoperability while degrading dependability and wasting spectrum. The right way to improve systems is to address all objectives together rather than piecemeal.

## ALTERNATIVE VISIONS

Within the overarching goal of developing a national broadband network, there are a number of possible paths forward. Allowing first responders to make use of multiple systems will increase the chances that some system is available and expand the capabilities that first responders can use. There should still be a primary system, which would at minimum support mission-critical voice communications, and possibly more.

Today, primary public safety communications systems are designed and run by thousands of independent local agencies, and this leads to interoperability failures, inefficient use of spectrum, lower dependability, and higher costs. One obvious response is to continue to rely

on government agencies but to move away from flexibility and toward standardization and a consistent nationwide architecture defined by one or more federal agency.

Even with a national architecture defined at the federal level, the federal government may or may not actually operate the infrastructure. Certainly, one option is for a federal agency such as the Department of Homeland Security (DHS) to deploy and operate the nationwide system. The government would pay directly for the infrastructure (although not necessarily for the mobile devices used by first responders that connect to this infrastructure). Another option is for local or regional entities to continue operating their own systems but to be required to design the systems so that they operate seamlessly within a national architecture. This approach is not unprecedented. For example, the Internet consists of many thousands of independent networks under separate administrative control, all of which operate and cooperate using protocols and architectures approved by the Internet Engineering Task Force. Similarly, many telephone companies around the world use consistent standardized technology.

One government program is already in place to develop a nationwide wireless network explicitly for law enforcement and homeland security. This network will be developed by federal contractors under the direction of the Departments of Homeland Security, Justice, and Treasury. The IWN will support 80,000 federal agents and officers. Even though it will be available to only a few percent of first responders— those from federal agencies—the network must still cover the entire country. The program is expected to cost between $3 billion and $30 billion.

One challenge in developing a nationwide system for all first responders is migrating from current systems without a disruption. This transformation becomes vastly simpler with the spectrum made available by the digital TV transition. Such a shift creates the opportunity to construct a nationwide system using some or all of that new spectrum and allows local agencies to gradually migrate from current systems to the new one over a period of years. As the agencies abandon their outdated technology and old spectrum allocations, some of these bands could become available for other uses.

Another approach to developing a nationwide system for serving first responders is to employ commercial companies. This approach has advantages. Multiple networks already operate in much of the country, and competition between these carriers drives costs down and quality up. However, commercial carriers rarely offer services designed to meet public safety standards for mission-critical communications. This is not surprising; most public safety agencies would not use these services regardless of their quality or price. Perhaps if they would, adequate services would emerge.

An alternative is to seek bids for a new nationwide system that would be specifically designed to serve public safety and would be run by a commercial provider. Many European nations have adopted this approach. For example, the British government has signed a contract with British Telecom to build a wireless system and operate it for 19 years. The system is intended for public safety, although it covers not just first responders but other public service agencies and even community health centers. Thus, the United Kingdom will gain the efficiency and dependability of a national system, with no possibility of interoperability problems, all provided through the existing expertise of British Telecom.

In the United States, Verizon is reportedly considering making a similar proposal, wherein the company would operate in 12 MHz of spectrum in the 700-MHz band that is currently intended for public safety after the digital television transition. Based on media reports, it appears that Verizon would serve public safety users only, in return for a fee. No spectrum or infrastructure would be shared with users who are outside of public safety.

Further efficiencies could be gained if a network serves both first responders and commercial users, where the former have priority. First responders need a system with great capacity during major emergencies, but most of the time they require little capacity, so capacity sits idle. Consumers can use this capacity. Cyren Call has requested 30 MHz in the 700-MHz band to establish just such a network in the United States. The network itself would be built and operated by a number of commercial carriers operating in different regions, while Cyren Call would be the network manager, setting service requirements, negotiating deals with equipment and service providers, overseeing compliance with requirements, and managing the flow of payments. Public safety agencies would pay for services on this network much as consumers pay for cellular services today.

The challenge when serving both consumers and first responders is to reconcile public safety's demands for dependability, security, and coverage with the public's demands for low cost. For example, a system serving only public safety would naturally be designed to maximize coverage, but a company deriving much of its revenues from commercial users will focus on population centers. Cyren Call proposes to bring terrestrial wireless coverage to 99.3% of the U.S. population, but to cover only 63.5% of the nation's total area—mostly urban areas—or 75% of the area within the contiguous states. (The company proposes using slower satellite communications to cover the remaining rural areas.)

---

## *CURRENT POLICIES ARE SO WASTEFUL THAT A POLICY CHANGE COULD EASILY REDUCE THE COST OF PUBLIC SAFETY*

*COMMUNICATIONS INFRASTRUCTURE, IN ADDITION TO SAVING LIVES AND SAVING SPECTRUM.*

---

The biggest challenge when many public safety agencies are served by a single commercial company is ensuring that the company has an incentive in perpetuity to provide good services at reasonable prices. If the only choices for public safety are to pay whatever this company asks or to discontinue wireless communications for first responders, then public safety is at risk. A traditional solution is to impose regulations on costs and quality, as is done with utilities. It is not clear whether such regulation would deter commercial companies, such as Cyren Call and Verizon, from entering this market. But there would be other, nonregulatory ways to mitigate this risk.

For example, individual public safety agencies have little power to negotiate with a nationwide company, so this task can be given to a single national entity, such as a federal agency or national consortium that represents all public safety agencies. The government also might require companies to sign contracts that clearly define performance standards across many criteria, including but not limited to dependability, security, coverage, and quality of service, so companies will not be rewarded for cutting corners. Contracts could run for long periods, so renewals can be negotiated well in advance. If a contract is not renewed, this leaves more time to create an alternative. In addition, the government might stipulate that public safety users do not have to pay for their last few years of service under a contract. If the contract is renewed, then payments continue without interruption. If not, the company must provide several years of services without payment, a situation that would increase the company's incentive to renew or enable public safety agencies to use the money they saved to prepare for whatever is next.

More extreme measures would make the company as dependent on public safety as public safety is dependent on the company. For example, when the government allocates spectrum to a company, the government can require that if the company fails to negotiate a deal acceptable to public safety, then the spectrum license is immediately revoked, even if the majority of the network's users are not associated with public safety. License renewal also could depend on input from DHS and other responsible public safety agencies. To go even further, the government might require the company to surrender its infrastructure to the next contract winner if the negotiation fails. Similar measures have been proposed for highly subsidized telecommunications providers "of last resort" in rural areas. Under this arrangement, there is no risk that vital public safety infrastructure will become unavailable, because it can always be reassigned. The challenge here is giving the company adequate

incentive to invest in infrastructure it could lose someday. Again, this requires long-term contracts and early negotiations.

In return for enacting provisions that protect public safety from monopoly service providers, the government might offer provisions that protect commercial carriers from other risks. For example, the government might guarantee that payments from public safety will not fall below a given level, even during the transition period when many public safety agencies are not yet making use of the new network.

Commercial companies also go bankrupt—especially new companies with innovative business plans. Contracts must address this possibility, so critical infrastructure will not be lost to public safety and there will be no disruptions in service. This problem is not new. Companies that operate other forms of critical infrastructure do go bankrupt from time to time, so there are models to follow.

The nation also has a variety of options to choose from in developing secondary systems to support first responders, assuming that the mission-critical voice communications are provided through a primary system. These possibilities are not mutually exclusive, so several could be adopted. The possibilities include:

***Cellular carriers.*** Cellular carriers can compete to offer services to public safety, and the diversity of current networks can greatly increase dependability and coverage, even if individual commercial networks do not always meet all of public safety's requirements. Cellular carriers also can provide new services that are not offered by the primary system.

---

*THERE IS NO REASON TO INVEST BILLIONS OF PUBLIC DOLLARS IN A NETWORK THAT SERVES ONLY FEDERAL FIRST RESPONDERS, WHEN THE VAST MAJORITY OF FIRST RESPONDERS WORK FOR STATE AND LOCAL AGENCIES.*

---

***A nationwide commercial carrier.*** As with the Cyren Call and Verizon proposals, a commercial company could provide services to public safety across the nation, but on a secondary basis, focusing on services such as broadband that are not widely available today to public safety. One such proposal comes from M2Z Networks, which has offered to provide free services to first responders in return for 20 MHz of spectrum near 2.1 gigahertz, which is less valuable than spectrum in the 700-MHz band. The company also pledges to provide broadband services to most of the nation's population and to return 5% of the revenues to the federal government. The company's network would cover 95% of the nation's population, so

presumably the percentage of area covered would be considerably less than that proposed by Cyren Call. Since the services are free, there obviously is no danger of M2Z Networks overcharging. However, it is still necessary to worry about whether public safety's service requirements will be met adequately and in perpetuity.

*Municipal infrastructure.* Municipal systems that blanket a city with wireless broadband coverage, or just serve strategically placed hot spots, are proving that they can play a useful role for public safety. These Wi-Fi–based municipal systems are relatively low-cost, provide high data rates, and can serve many needs, including but not limited to public safety. Although this technology is currently not capable of providing some mission-critical applications over a large region, it is fine for certain uses. These uses include fixed applications, such as transferring data from a remote surveillance camera to a command center, and applications where lives do not depend on ubiquitous and instantaneous access, such as transferring arrest reports from a police car back to the station.

*Ad hoc networks.* Ad hoc networks are ideally suited for applications where all devices are mobile or are transported to an emergency as needed. Such networks might be set up quickly among portable devices placed in a burning building or among fast-moving police cars. This is also an effective solution where much of the communications is local— for example, to enable public safety devices operating within an urban subway system to communicate with each other at high data rates.

*Satellite networks.* Satellite systems can cover vast regions and are largely immune from earthquakes, hurricanes, and most terrorist attacks. Thus, they may play an important role in sparsely populated areas where terrestrial coverage can be expensive, or in areas where terrestrial systems have been destroyed by a recent disaster. However, they are generally not the first choice where good terrestrial options are available. The time it takes a signal to travel to a satellite and back is inherently problematic for some applications, including basic voice communications. Today's mobile satellite devices tend to be more expensive, larger, heavier, and more power-hungry than their terrestrial counterparts, which makes the satellite devices less attractive for many first responders.

## NEXT STEPS

The challenge, of course, will be in devising public policies that will help reach these goals. If the nationwide broadband system is to be run by a commercial company, a number of complex issues must be worked out with the companies that come forward. If the system is to be run by government entities, policymakers could begin the process today. This latter process is essentially the same regardless of whether the network will ultimately be run by one federal

entity or a collection of local or regional entities. The best approach would be for policymakers to pursue both paths in parallel.

The first step is to establish the technology and architecture for a nationwide broadband network that will meet the long-term needs of public safety. The Federal Communications Commission (FCC) and DHS would presumably have roles to play in this process, with plenty of input from public safety organizations, equipment manufacturers, wireless service providers, and other stakeholders, as well as from disinterested experts. The process itself should resemble the development of an open standard more than the typical rulemaking of a regulatory body or the opaque pronouncements that are possible from an executive-branch agency. Ultimately, an architecture should be adopted that is based on open standards, for which no entity (other than the federal government) owns intellectual property. It would include a broadband backbone, which is likely to be based on the versatile Internet protocol (IP), and standards for wireless communications. It would incorporate gateways to legacy public safety systems, as well as potential secondary systems such as commercial cellular carriers, municipal Wi-Fi systems, ad hoc networks, and satellite systems.

Given the stakes of such a fundamental shift in public safety infrastructure, the government should take the time to consider a variety of current and emerging technical options and to seriously investigate the long-term implications of each. Thus, the government should provide funds to such agencies as the Homeland Security Advanced Research Projects Agency and the National Science Foundation specifically to engage forward-looking researchers outside of government, much as it has used the Defense Advanced Research Projects Agency when considering major shifts in technology for military use.

It also is time to reevaluate the IWN. There is no reason to invest billions of public dollars in a network that serves only federal first responders, when the vast majority of first responders work for state and local agencies. One possibility is to greatly expand this program so that it supports all first responders. But if such a vast change in scope is not practical, then the network should be shelved so funding can be reallocated to a more complete solution to the problems of communications for public safety and homeland security.

Either the FCC must make spectrum available for this network, presumably at 700 MHz, or the Department of Commerce must make the IWN spectrum available for this purpose . Assuming the former, this need not increase the total amount of spectrum going to public safety, but it does mean that the FCC must abandon the policy of granting local public safety agencies maximal flexibility regarding the use of spectrum at 700 MHz. None of the proposals for spectrum allocation currently before the FCC meets this requirement.

If the nationwide network is to be government-run, the federal government must provide funding to build the nationwide infrastructure, although much or all of the funding for the

mobile devices held by first responders might come from local agencies. In the long run, the money saved by an efficient system should be far greater than the amount spent, but not during the initial transition period. One possible source of funds is auction revenues from the TV spectrum that will be allocated for commercial use.

In parallel with pursing the path toward a government-run nationwide infrastructure, serious attention also should be given to the proposals of the commercial companies Cyren Call, Verizon, M2Z Networks, and perhaps others to come. A commercial public safety network may have the potential for greater benefits than a government-run system. This is especially true if the network also serves users outside public safety, so the system can be put to good use between emergencies, leading to much greater efficiencies in the use of expensive infrastructure and scarce spectrum. However, a commercial system also carries greater challenges and risks. In particular, the government must take steps to ensure that commercial companies will meet public safety's requirements, including requirements for coverage, dependability, and security, and that requirements and fees can safely evolve over time as technology and needs change. Commercial companies will have strong incentive to cut costs and raise prices where they can, and public safety may be in a poor position to negotiate. Moreover, commercial companies that hope to derive their profits from paid subscribers will naturally try to avoid serving sparsely populated areas. It is not clear yet whether these issues can be resolved to the satisfaction of all. None of the proposals to date are sufficiently specific to address these issues. Because the risks and rewards of this approach are both great, more detailed consideration of these proposals is warranted.

Regardless of whether public safety's new nationwide network is operated by government or a commercial company, if it serves only public safety, then the spectrum allocated to this network will sit idle much of the time. Instead, the spectrum should be shared with another user who would have secondary access. Given that public safety would not need the spectrum often, secondary rights might be auctioned for almost as much as dedicated spectrum. Thus, for example, if public safety had exclusive access to 12 MHz and primary access to 24 MHz that is shared with commercial systems, then this might be far better for both public safety and commercial users than giving public safety exclusive access to just 24 MHz. This could also generate greater auction revenues.

Because commercial carriers could play a more important role in public safety, either as primary or secondary service providers, the government should adopt policies that would increase their dependability. Policymakers should first provide market incentives for carriers to be more dependable. Carriers are rewarded for investing in better service only if customers are willing to pay more as a result. Today, customers cannot know which carrier provides the most dependable service, with or without a major disaster, so no one will pay more for a dependable service. If the FCC released annual report cards on each commercial carrier's