

March 15, 2003

Interoperability issues jeopardize homeland security

Technological and economic limitations prevent communication between public-safety agencies

As the nation mourned the loss of life in the terrorist attacks of September 11, a gut-wrenching fact came to light: warnings about the Twin Towers' imminent collapse failed to reach many emergency responders because of communication problems. Police helicopters above the World Trade Center radioed their concerns about the buildings' stability 21 minutes before the South Tower fell, giving rescuers ample time to escape. Hundreds of firefighters, however, did not receive that warning because they were using a different radio system. Subsequent interviews and inquiries appeared to indicate that this inability to communicate played at least a partial role in the deaths of 343 firefighters at the World Trade Center.

Although this scenario represents the most drastic circumstances ever faced in the United States, lack of "interoperability"—the ability of public-safety service and support providers to communicate and exchange data—presents a significant threat to homeland security. The reasons behind this critical issue cover a broad spectrum: incompatible hardware; agencies operating on frequencies too far apart for other radio equipment to pick up the signal; limited radio channel availability; interference from cellular telephones sharing the same airwaves. Regardless of the cause, the result remains the same—lives jeopardized because emergency commanders cannot communicate with all responding agencies.

The tragedy of September 11 focused a spotlight on this problem, which has existed for years and continues to persist today. In the aftermath of the Oklahoma City bombing in 1995, for example, couriers had to carry messages on foot between agencies that could not communicate with each other via radio. The necessity of different agencies to exchange information at all levels, from senior leadership to new recruits, transcends the occasional terrorist act, applying to natural disasters, domestic crime and automobile accidents as well.

Scope and history of the problem

Concerns about the lack of interoperability among the nation's first responders have been voiced in many public arenas. "America—Still Unprepared, Still in Danger," an independent report commissioned by the Council on Foreign Relations (CFR) and led by former Senators Gary

Hart (D-Colo.) and Warren B. Rudman (R-N.H.), singled out communication difficulties as one of "the risks that the United States still confronts." Released in October 2002, the report asserts that "in virtually every major city and county in the United States, no interoperable communications system exists."

The communications rift began widening in the early 1980s with the advent of new technology. Increasing advancements flooded the marketplace with a wide range of communications options in radios, cellular telephones, pagers, etc. This helped to broaden the problems between agencies' communications systems. In addition, separate budgets and rivalries between departments often lead to fire and police departments using different equipment incompatible with each other as well as with neighboring jurisdictions. The disjointed communication that results can impede effective, efficient responses by public-safety agencies, which can risk lives even in routine traffic accidents. In a natural disaster or terrorist attack, the consequences could again be catastrophic.

Without the ability to share information through radio systems, first responders may reach a disaster scene unprepared to address the situation. Redundant steps performed by different groups may waste precious time, while other areas of need may suffer from unintentional neglect. Emergency response agencies throughout the country have experienced the complications that result from the incompatibility of radio systems, ranging from frustrating nuisances to life-threatening obstacles.

- As police, fire and medical units rushed to the scene of the Columbine High School shooting in Littleton, Colo., few of them could communicate due to a morass of different radios on different channels across the spectrum.
- While responding to a flood in the Midwest, members of the National Guard and other rescuers resorted to shouting to each other across

(continued on next page)

Interoperability issues jeopardize homeland security

Technological and economic limitations prevent communication between public-safety agencies

(continued from preceding page)

a rain-swollen river due to a lack of connection between their radios.

- At the Pentagon on September 11, three Virginia response units—fire departments from Arlington, Alexandria and Fairfax—had all worked together routinely and shared a common radio system. Agencies from Washington, D.C., and Maryland, however, had to borrow spare radios from the others to keep informed and then had to relay all the information to their rescuers through their own systems.

The obstacles to developing a comprehensive shared communication network between emergency responders throughout the United States—tight budgets, lack of uniform standards—present a daunting challenge. Without a seemingly plausible solution, many local departments acknowledge the potential problems but have no plan of action, while others have created makeshift methods of coping with the situation. Some agencies relay messages to neighboring districts by signaling local radio dispatchers who then telephone dispatchers in the targeted area to share the information.

Technological advances

Although no official standard exists, technology to overcome interoperability problems is available. In fact, a range of technological advances offer options at varying price levels to address this issue.

Modular interconnect systems. JPS Communications, Inc., a subsidiary of Raytheon, has developed a system that converts communications traffic to its essential elements: the reception and transmission of audio signals and the ability to control the diverse array of communication devices used by emergency responders. Approximately the size of a VCR, the interconnect system unites up to 12 communication devices, translating information received on one frequency for transmission on another. In Washington, D.C., the dispatch center of the

Arlington Police Department uses two of these systems to link 16 different radios used by a dozen different agencies. As each radio receives a signal, the interconnect unit translates the message into a form that can be broadcast to other systems—usually with a lag time of less than one second. At an estimated price tag of \$10,000 to \$30,000 per unit, this system represents a reasonably inexpensive, but effective, method of resolving the interoperability challenge.

800 MHz radio systems. Digital 800 MHz radio systems can significantly improve interoperability between public-safety agencies. The high-frequency radio systems offer several advantages. First, the higher-bandwidth channels have less traffic and are therefore less likely to become clogged during an emergency. “Trunking” technology further reduces the chances of overloading the system by allowing multiple transmissions to occupy the same frequency space. Unlike VHF, which dedicates a single channel to a specific group of users, this technology enables allocation of the radio frequency spectrum as needed. When communicating via the trunked radio system, it automatically finds an available channel, and then relinquishes it to other talk groups at the end of the conversation. This system simultaneously broadcasts the same information from every repeater antenna or site. Public agencies thus share the same infrastructure, although each has the ability to communicate privately with its own personnel. Another advantage of this system is that it improves security by making it virtually impossible for an outside party to intercept the information.

Unfortunately, many challenges prevent widespread implementation of these systems. Competing manufacturers offer variations of this technology, which are not entirely compatible with one another. Also, local agencies operate on independent budgets and timetables with regard to their respective communication systems. A city police department, for instance, may replace its system with new technology having a life expectancy of 20 years, but the fire department

budget in that same jurisdiction may call for retaining its existing, incompatible system for another 10 years. Furthermore, the costs of this technology put it beyond the reach of many agencies. The radios themselves cost three to four times more than radios for analog systems, and the infrastructure required for the networks demands a multimillion-dollar investment. One important advantage, however, lies in the fact that once funding is obtained for this initial investment, public agencies in the surrounding area need only pay for the radios.

On-site communication vehicles. Following the explosion of the space shuttle last month, Raytheon deployed for the first time a mobile communications system to assist with the recovery of the debris. The system, which was developed after the terrorist attacks of September 11, 2001, combines the interconnect units described above, satellite links and sophisticated computer technology to unify incompatible communication systems. No modifications or upgrades to existing systems are necessary. The components are installed on sports utility vehicles, at a cost of \$250,000 to \$300,000 apiece. The manufacturer has already sold 15 of the units, including one scheduled for delivery to the Los Angeles Sheriff's Department this month, and expects to sell an additional 50 to 60 systems in the next six months.

Obstacles to interoperability

Although several technological solutions exist that can remedy this problem, significant obstacles to their implementation remain.

Funding. As mentioned above, lack of funding poses the greatest challenge. Even the most affordable options are still more expensive than many budgets can sustain at present. Last spring, the Public Safety Wireless Network (PSWN) program—a federal initiative to promote communications interoperability—conducted two one-day conferences to identify the primary challenges hampering wireless interoperability and to develop solutions to overcome these

obstacles. Both events focused on proposals that would facilitate statewide communication among public-safety agencies. “Cost-effective” solutions still carry a price tag of millions of dollars, and federal funding, while generous on paper, has proven scarce in reality.

Lack of standards. A set of standards currently exists but desperately needs to evolve. As manufacturers of wireless communication devices have enhanced the functionality and efficiency of their products, they have also exacerbated the need for standards. The new technology typically uses unique, proprietary protocols that are incompatible with other companies' systems.

Manufacturers cite several reasons for their reluctance to embrace existing standards. Some argue that full standards compliance is too expensive because of the licenses required to purchase the intellectual property rights associated with the standards. Others claim that adhering to current standards carries too much risk because standards continually evolve according to technological changes and users' needs. Even so, many manufacturers have played an instrumental role in developing standards and deserve credit for the progress made so far.

More progress is needed, however, particularly given the nation's heightened risk of terrorist attack. The current set of standards needs to evolve, addressing new technologies such as trunking and encryption and applying to infrastructure components. Now, proprietary protocols require that radio infrastructure components for a system must come from a single supplier. If an agency needs to join a network or expand coverage within the existing system, it must purchase the new equipment from the original supplier. The lack of competition results in higher prices and fewer consumer choices.

Geographical challenges. As mentioned above, the 800 MHz radio systems currently used to great effect by many of the nation's large metropolitan

(continued on next page)

Interoperability issues jeopardize homeland security

Technological and economic limitations prevent communication between public-safety agencies

(continued from preceding page)

areas require the construction of an extensive infrastructure—the costs of which are prohibitively expensive in rural areas of the nation. Less-sophisticated solutions can often accomplish the goal with equal efficacy in these regions. As one example, a county sheriff in the Rocky Mountains keeps a cache of extra radios for responders in neighboring jurisdictions to use when engaged in joint operations with his deputies.

Densely populated areas that can efficiently use the infrastructure are encountering yet another problem: lack of spectrum availability. The evolution of technology has made the radio spectrum an increasingly scarce and valuable commodity as more and more electronic devices require it for their operation. The Federal Communications Commission (FCC) regulates the use of frequencies, allocating certain portions of the spectrum for the specific use of public-safety agencies. To address the growing need for spectrum dedicated to public safety, the U.S. Congress has allocated an additional 24 MHz of the radio spectrum in the 700 MHz band to public safety. Radios operating in the 700 MHz band will be interoperable with the existing base of 800 MHz band users. However, this reallocation depends upon the relocation of analog television channels to digital television (DTV) and the availability of equipment that can access DTV signals, and it will likely not come to pass for several more years.

Labor and time intensity. Even overcoming the previous obstacles, upgrading all of the nation's public-safety agencies to a unified, interoperable system poses a tremendous challenge. Simply building the infrastructure for such a system would require years—and billions of dollars. "You're not quite reinventing the wheel," says one federal law-enforcement expert, "but you're coming close."

To assist in this effort, the federal government created the AGILE (Advanced Generation of Interoperability for Law Enforcement) program

in 1998, pulling together all interoperability efforts within the National Institute of Justice and serving as the contact point for coordinating interoperability initiatives. AGILE has four primary components: the support of research and development, the evaluation and piloting of technologies, standards development, and education and outreach. This initiative represents an important step in examining the problem of interoperability and developing solutions, but the ultimate resolution of this critical situation will demand commitment from user groups and close cooperation and open communication between policy-makers and equipment manufacturers.

The lack of a unified communications system among the nation's emergency responders poses a significant threat to homeland security. The problem has been identified, its consequences tragically demonstrated in countless scenarios, from automobile accidents to the tragic deaths of firefighters in the collapse of the World Trade Center. Technology to remedy the situation exists, and budget supplements for security—while slow to reach the appropriate agencies—continue to receive government approval.

America should not run the risk of lapsing into complacency. Safety and security must remain top priorities as the United States faces the ongoing war against terrorism, a potential war with Iraq and a tremulous economy. Government officials, business leaders and private citizens alike must sound a call to action and address the deficiencies in our homeland defense that still exist more than 16 months after the worst terrorist attack in U.S. history. In an emergency situation, information sharing plays a critical role in saving lives—an inability for first responders to communicate is simply not an option.



The Lipman Report Editors