International Journal of Communications Law and Policy

Issue 7, Winter 2002/2003

EMERGENCY COMMUNICATIONS: THE QUEST FOR INTEROPERABILITY IN THE UNITED STATES AND EUROPE

Viktor Mayer-Schönberger*

Late in the morning of April 20, 1999, Eric Harris and Dylan Klebold, two sixteen-year-old students, entered Columbine High School and started a shooting spree that would leave fifteen people dead, including Harris and Klebold, and dozens of others wounded.[1]

Within minutes of the first shootings, local police, paramedics, and firefighters arrived at the scene. Over the next several hours, they were joined by almost 1,000 law enforcement personnel and emergency responders. The task they faced was daunting. They did not know the number of attackers, their location, or the goal of the attack. Hundreds of screaming students were fleeing the school; many others were trapped in it, deadly frightened and waiting to be freed. Scores of people were wounded and needed immediate medical attention. Seventy-six bombs and explosive devices set up by Harris and Klebold had to be identified and defused.

Yet as it turned out, the biggest challenge on that Tuesday afternoon was not battling the two attackers. They had already killed themselves when the first law enforcement team entered the

* Assistant Professor of Public Policy, The John F. Kennedy School of Government, Harvard University. This research was supported by the Executive Session on Domestic Preparedness. This was to be a coauthored paper with my colleague Richard Falkenrath, now Special Assistant to the President and Senior Director for Policy and Plans with the Office of Homeland Security, who convinced me to look at interoperability. He deserves much of the credit for this paper. Deborah Housen-Couriel provided truly exceptional research assistance. Anatole Papadopoulos helped to track down hard-to-find sources in the final stages of the project. I am most grateful for many suggestions from Arnold Howitt and Robyn Pangi of the Executive Session on Domestic Preparedness, as well as David Lazer, Thomas Oberlechner, Robert Heverly and Gernot Brodnig for reading and extensively commenting on earlier drafts. I am especially grateful to Herbert Cordt for demonstrating that networks are not just technical artifacts, and to Werner Senn, Herbert Nagy, and numerous interview partners in the Burgenland for generously taking time to answer my queries.

[1] The description and analysis of the Columbine High School incident is based on the John F. Kennedy School of Government Cases "The Shootings at Columbine High School: Responding to a New Kind of Terrorism," Case No. C16-01-1612.0, and "The Shootings at Columbine High School: Responding to a New Kind of Terrorism Sequel," Case No. C16-01-1612.1.

school. The biggest challenge was coordinating heavily armed and ready-to-fire police forces from half a dozen sheriff's offices and twenty area police departments, forty-six ambulances, and two helicopters from twelve fire and EMS agencies, as well as personnel from a number of state and federal agencies. Coordination was difficult not primarily because of turf wars or lack of crisis management. If anything, first responders, some of who had taken part in Federal Emergency Management Agency (FEMA) training, were quite willing to work with each other.

The real challenge was simpler—and much more serious. Responders from the various agencies had no communications system that would permit them to communicate with each other. Agencies used their own radio systems, which were incompatible with those of others. With more and more agencies arriving on the scene, even the few pragmatic ways of communication that had been established, like sharing radios, deteriorated rapidly. Cellular phones offered no alternative, as hundreds of journalists rushed to their phones and overloaded the phone network. Within the first hour of the operation, the Jefferson County, Colorado, dispatch center lost access to the local command post because the radio links were jammed. Steve Davis, public information officer of the Jefferson County Sheriff's Office, later commented that "[r]adios and cell[ular] phones and everything else were absolutely useless, as they were so overwhelmed with the amount of traffic in the air."[2] The real miracle of Columbine High is that nobody else got killed because of the complete communications breakdown, either through friendly fire or uncoordinated agency activity.

Yet the communications breakdown was to be expected. Analysis of the 1993 World Trade Center bombing, the 1995 Oklahoma City bombing, and the standoff between the Federal Bureau of Investigation and Branch Davidians in Waco, Texas, in 1993, in which nearly 100 people died, all pointed to interagency communications as one of the weakest links in emergency management. In the immediate aftermath of the Oklahoma City bombings, for example, the four radio channels available to the Oklahoma City police department instantly became congested.[3] Only one of a total of two channels accessible to the fire department was available for rescuers, as the other channel had to be used to manage all other Oklahoma City fire coverage. Initial communication with the com-

[2] "The Shootings at Columbine High School: Responding to a New Kind of Terrorism," p. 16.

[3] Public Safety Wireless Network (PSWN), Program Symposium Compilation Report, August 1997–December 1999, pp. 19–23

mand post took place via cellular phones, until cellular phone networks, too, became overloaded. Similar miscommunication hampered emergency responses to the Amtrak train derailment in Arizona in 1995 and the Florida forest fires in 1998.[4] After each tragedy the need for interoperability, for linking communications networks of the various agencies, was a significant issue. The lessons were visible for everyone in the field. Still nothing fundamentally had changed by 1999, the year of the Columbine tragedy.

Interoperability is "the ability of public safety personnel to communicate by radio with staff from other agencies, on demand and in real time."[5] Public safety agencies have used radio communicationssystems for many decades.[6] So far, however, most of these systems have been limited in reach and have enabled communication within a particular group or agency, but not across agencies. A group of firefighters, for example, can talk among themselves over their radio, but not with paramedics or law enforcement officers, and sometimes not even with fellow firefighters from a neighboring town or county. This severely curtails the utility of radio communications, especially in situations that demand large-scale immediate interagency communication and coordination.[7]

This is an essay about communications interoperability and its implementation, here in the United States and in Europe. Three steps have been seen as requirements for interoperability: inventing the appropriate technology, setting common standards and frequencies, and providing adequate funding.[8] This essay looks at each of these steps in the U.S. and European contexts and analyzes successes and failures, rendering a fuller picture both of the challenges for interoperability and of best practices to meet them. Over the last few years (and surprisingly given the complex political structures) the Europeans have pulled ahead of the U.S. in implementing interoperability,

[4] Ibid.

[5] PSWN, *Public Safety and Wireless Communications Interoperability—Critical Issues Facing Public Safety Communications*, p. 1.

[6] The Detroit police department was the first to use mobile radio receivers in the 1920s; radio transmitters followed in the 1930s. See The First Two-Way Police Radio Systems, The Philip B. Petersen Collection (July 2, 1989) available online at http://www.infoage.org/p-29Police.html.

[7] Interoperability concerns of communications networks in the public sector are not limited to public safety organizations. The military, too, has grappled with the problem. See only Anthony W. Faughn, *Interoperability: Is It Achievable?*, Program on Information Resources Policy (PIRP) Working Paper (Cambridge, MA., September 2001).

[8] In addition to these three steps PSWN, *Public Safety and Wireless Communications Interoperability—Critical Issues Facing Public Safety Communications*, mentions security as an additional obstacle to interoperability.

structures) the Europeans have pulled ahead of the U.S. in implementing interoperability, although with determination and the right set of strategies, U.S. policymakers can easily make up lost ground. Enhanced Federal Communications Commission (FCC) leadership in defining frequencies and standards and a clearly formulated and thoroughly executed comprehensive funding strategy, based either on public funds or innovative public-private partnerships, would go a long way toward enabling communications interoperability to take hold.

But this essay is not simply about how to overcome obstacles on the path to interoperability. The case of interoperability, its elusiveness in the United States and its successes elsewhere, reveals a deeper, more troubling story—a story not so much of technical hurdles, as of structural and political hurdles, as more of perceived than actual constraints, unduly limiting the nation's ability to cope with an important public policy need. There are no abstract silver bullets to overcome the problem. Instead, policymakers have to look carefully at how well the policy strategy they select is aligned with their means and the policy context. In the United States, interoperability has suffered from strategic misalignment and haphazard implementation. European interoperability policies have fared better, not because of a general advantage in the strategies chosen, but because of a better fit between means and ends. Interoperability provides an intriguing test case, highlighting the transcending importance of strategic alignment, agency innovation, and leadership.

I. The Path toward Interoperability—and Its Three Obstacles:

Over the course of the last decade, numerous public- and private-sector organizations have studied interoperability and the difficulties involved in achieving it.[9] Three general obstacles that need to be overcome to establish interoperability emerge from these studies: finding a suitable technology; defining a common frequency and standard; and securing the necessary funding. These obstacles may reinforce each other, rendering the triad potentially even harder to tackle than they would be as individual barriers.

[9] See for example PSWN, *Public Safety and Wireless Communications Interoperability*; National Institute of Justice, *State and Local Law Enforcement Wireless Communications and Interoperability - A Quantitative Analysis* (January 1998); European Radion Commission, Harmonisation of Frequencies for Police and Security Services in Europe, ERO Report no. 6 (1991).

As an example, suppose five people speaking five different languages want to communicate with each other. First, they have to understand that every one of them is capable of learning a new, common language. In the interoperability context, this represents the technical hurdle. The next step is to define this new language, its grammar and its vocabulary. This is the frequency and standards hurdle. Finally, they need to have the resources available to actually learn this new language. This represents the third hurdle, the need for appropriate funding. Obviously, overcoming one hurdle is necessary to overcome the next, but it does not make overcoming the next hurdle any easier, as each hurdle has its own unique difficulties. Worse, focusing energies on overcoming one hurdle may divert necessary resources to tackle the next thus making it harder to overcome all three of them together.

(a) Finding a Suitable Technology

A truly interoperable public safety communications network will have to integrate the radio networks of local law enforcement, firefighters, EMS, and other local, state, and federal public safety organizations. It will also have to accommodate the communications systems of neighboring public safety agencies, so that officers from one locality can talk with their colleagues in others. Hence hundreds, even thousands of users will have to be linked through a network extending beyond states and even nations.

Conventional analog radio equipment is ill-equipped to perform this integration task because it does not scale well. Participants using such equipment converse on a specific channel. The ability to speak and listen is shared among all the users. Multiple users cannot speak simultaneously. This limits the amount of information that can be exchanged. Adding channels eases the problem only temporarily, as extra channels require more bandwidth and hence a broader radio spectrum dedicated to public service communication. Radio spectrum, however, is not a boundless resource and must be shared with many other user groups. Moreover, even if bandwidth were endless and an unlimited number of extra channels available, managing who uses what channel with whom for what purpose poses a substantial coordination problem. In an emergency like the Columbine High School case, there is no time to sit down and coordinate rationally among the emergency responders

how channels are used. Emergency planning and preparation may reduce the coordination problem, but it cannot prepare for all contingencies.

Interoperability requires a technology that scales, can accommodate many thousands of users efficiently, and can coordinate among them automatically to utilize best the scarce resource of channels available, while offering better voice quality and perhaps even additional services like data transmission. A simple walkie-talkie is hopelessly inadequate to fulfill these requirements. Yet almost all of the emergency responders in the United States today use equipment that differs little from traditional two-way radios.

(b) Defining a Common Frequency and Standard

Once a suitable technology for interoperability has been identified, its success depends on its employment of a common frequency and standard. Without such commonality, even the best technology will be useless in terms of interoperability, and for an obvious reason: A common frequency allows all users to communicate over the same set of channels. Trying to communicate over different channels when each party has access to only her own channel is like attempting to watch channel 3 with a TV set that receives only channels 5 and 6.

Understanding the need for a common frequency is intuitive, but meeting that need is hard. Various public service agencies, from law enforcement to firefighters to EMS, have traditionally used different (and limited) frequency bands for their radio communications.[10] For interoperability to work, a sufficiently broad spectrum needs to be set aside for it.

Even a common frequency, however, is not enough to establish interoperability. It requires not just a common frequency band but also a common standard, a common implementation of a selected

[10] Thirteen discrete portions of spectrum are currently allocated for public safety operations, including the 25-50 MHz, 72-76 MHz, 150-174 MHz, 220-222 MHz, 450-470 MHz, 470-512 MHz, 764-776 and 794-806 MHz, 806-821 and 851-866 MHz, 821-824 and 866-869 MHz bands for state and local agencies, as well as the 30-50 MHz, 138-150.8 MHz, 162-174 MHz and 406.1-420 MHz bands for federal agencies; see PSWN, *Spectrum Issues and Analysis Report* (1999).

technology. For example, many cellular phones in the United States use a common frequency band, the 1900 MHz band. Still, users from one cellular phone operator cannot call through the network of another and could not even if both operators wanted, because although the networks use the same frequency band and the same basic technology platform (digital wireless), the concrete implementation of the technology differs among operators. Cellular phone operators use one of three competing standards,[11] so cellular phones are wedded to a particular operator's network, whether the users or even the operators like it or not.[12] They are not interoperable, even though they operate over a common frequency.

(c) Securing Necessary Funding

Even if the appropriate technology is identified, and a common frequency and standard selected, it is very unlikely that interoperability will happen overnight. For interoperability to be implemented, all existing radio communications infrastructure used by public service agencies must be substituted with new equipment. This involves more than just replacing the hundreds of thousands of radio sets currently in use. Every one of these agencies also operates a small radio network consisting of dispatcher stations, transmitters, and relay stations to link the individual radio sets with each other and with the command post, and this network infrastructure needs to be replaced as well. In addition to the new hardware (i.e., the radio sets and networks) hundreds of thousands of users may need to be trained to use the new equipment. Finally, this transition must take place in real time, while emergencies continue to happen that require first responders to be in active communication.

---

[11] The current standards for digital cellular phones used in the United States are TDMA, CDMA, and GSM. In addition, some cellular phone operators still maintain analog networks.

[12] Technical interoperability must not be confused with whether network operators actually permit interoperability. All cellular phone operators permit interoperability in the sense that any cellular phone user can call (and be called) by anyone on the global phone network as long as they are within range of their cellular operator's network. Yet few cellular phone operators in the United States permit other operators' cellular phone users to temporarily use their networks. Experts call this flavor of interoperability "roaming." "Roaming" could be mandated through regulatory action, but only if operators used the same technology, standard, and frequency.

Such a large-scale shift to an interoperable infrastructure is a logistical challenge, in however staggered a fashion it may take place. Yet, the logistical challenge pales in comparison to the financial challenge. Studies have estimated that the total replacement value of radio equipment used by public service organizations in the United States exceeds $18 billion. More than 80 percent of the cost of replacement will have to be shouldered not by federal or state, but local agencies.[13] This amount does not include the cost of training and practice. Moreover, every one of these tens of thousands of individual organizations will make its own procurement decision, based on its own preferences as well as available funds.

Interoperability may have a chance only if all three of these obstacles—technology, common frequency and standard, and funding—are overcome. Surmounting these obstacles is what some studies and reports have deemed the fundamental challenge for interoperability.[14]

II. Growing Hurdles: U.S. Policy toward Interoperability

Comprehensive communications interoperability among public safety agencies has been a long–standing goal of U.S. policymaking, reinforced by the tragedies of Oklahoma City and Columbine High. Early on, experts identified the three hurdles that needed to be overcome, and significant effort was expended to dismantle them. How successful was this strategy?

(a) Technology: Success of Innovation

Interoperability, as mentioned earlier, requires a technology that scales well and is capable of simultaneously accommodating many users, given the constraint of limited radio spectrum bandwidth. Technology's central task is to use the available bandwidth as efficiently as possible.

---

[13] See PSWN, *LMR Replacement Cost Study Report* (June 1998), p. 5.

[14] See for example PSWN, *Public Safety and Wireless Communications Interoperability*; National Institute of Justice, *State and Local Law Enforcement Wireless Communications and Interoperability* (January 1998); European Radio Commission, *Harmonisation of Frequencies for Police and Security Services in Europe*.

To increase the efficiency of bandwidth use, a communications network can take over the task of allocating channels for communications. Instead of human users flipping through channels and determining manually whether a given channel is "free" to be used, technology manages the assignment of these channels. Such assignment can be made based on a first-come, first-served system. When all available channels are in use, technology will—once a given conversation is over—automatically deallocate the channel used for that conversation and assign it to the users next in line for a free channel. Unlike cellular phone conversations, most communication on public service networks tends to be short, permitting a high turnover rate and relatively short waiting times.

Such a system offers the substantial advantage over systems currently in use of eliminating the need to designate a particular channel for a particular use. There need no longer be a dedicated "dispatcher" channel, or a "group channel" for each team or group. Instead, network technology takes any request for a channel, finds a free one, allocates it, and establishes the connection. This is in essence what cellular phone networks do today. Only a limited number of channels are available, and the network automatically assigns them to users requesting to communicate.

Unlike cellular phone callers, however, users of a public service network typically cannot wait many seconds for the network to designate a channel for them. Instead, they require instant communication setup. In addition, networks allocating channels based on temporal priority—first come, first served—are not ideal for public service organizations. Channel allocation in such organizations should not be based on who asked first, but on whose communication need is most important. A police officer requesting a channel to communicate a routine status report should not get priority over her colleague's emergency call for mutual assistance just because her request was received first. A suitable network technology must assign channels based primarily on communication needs.

This implies a network capable of managing itself, understanding requests, allocating and deallocating channels, and keeping on top of the traffic on the network. Public service organizations striving for interoperability require "intelligent" digital networks that are far more sophisticated that the radio networks currently in place. Such digital networks translate all communications into a unified digital code before routing them through the network. On the receiving end, bits are translated back into, for example, voice communication. The advantage of employing such a digital code

is that the network can "manage" it easily. This is why interoperable public service networks are based on digital technology.

Digital networks receive communication requests from users along with information about the importance of the communication and queue the requests accordingly. Emergency communication requests get prioritized and may even prompt the network to deallocate the lowest-priority communication under way, in effect kicking off users for an incoming emergency communication—a capability available neither in conventional analog radio networks nor in digital cellular phone networks. Digital technology also permits the compression of voice transmissions. Compressed transmissions in turn decrease the amount of data that needs to be transferred for the same communication, and less data requires smaller channels (less frequency bandwidth), for example by compressing voice into a 6.25 kHz instead of a 25 kHz channel. Hence, more channels can be fit into a given frequency band.

Managing channel allocation generally points toward a network technology with a strong center, a kind of superfast dispatcher in charge of assigning communication rights to users. Networks that employ this kind of technology are called "trunked" networks, implying that they have a strong trunk, or center, managing them. Yet efficient network management can also be based on a decentralized structure. Instead of being managed by a core, the network parts automatically coordinate the use and management of the network's resources among themselves. The Internet is such a network. The advantage of such a network is that it provides for ample redundancy. Even if a part of the network stops working, the rest will continue to operate. Trunked networks, on the other hand, will stop working if the managing center has been brought down. The advantage of decentralized networks, however, comes at a price. They require a much higher coordination overhead. Establishing a connection demands valuable time in decentralized networks: the more network links are involved, the greater the time required. This runs counter to one of the central requirements of emergency responder networks: instantaneous communication setup.

Long setup times, however, are inherent in current decentralized networks. Unless this deficiency can be overcome by some next generation technology in the future, every decentralized network is plagued with this problem. On the other hand, trunked network's Achilles Heel – what to do in case the center is taken out – can be mitigated. For example, trunked networks can operate a

backup core that takes over instantaneously in case the primary network core fails. Of course, such redundancy comes at a cost. A second transmitter and digital dispatch unit has to be procured, and primary and backup dispatch units have to be linked by a data channel so that they can continuously synchronize traffic management. Adding more such cores further enhances redundancy, but increases the data traffic overhead. One could also keep a special mobile backup transmitter and dispatch unit ready, and only deploy it on the ground (by helicopter or other means) in case the primary fixed core has failed. Trunked network equipment suppliers have successfully implemented such a possibility, which not only adds redundancy but also is capable of rapidly deploying trunked network capability wherever it is needed. Another strategy is to build into radios for trunked networks functionality to talk directly with each other even without a core. Of course, that way one looses much of the advantage of efficient channel management, but rudimentary call prioritization may remain, thus providing a backup solution superior to existing analogue networks. None of these measures will rid completely a trunked network of its Achilles Heel, but when combined they will drastically reduce the risk that taking out a core in a trunked network may render the communications infrastructure useless.

On balance, hence most experts today advocate the use of digital trunked networks rather than decentralized networks to provide scalable interoperability for public service organizations.[15] They think that the chance of a trunked network failing because its center has stopped working is small and thus a good trade-off (especially factoring in backup centers and similar resources) compared to unacceptably long communication setup times associated with decentralized networks.

(b) Common Frequency and Standard: Out of Synch with the Present

The process of defining a common frequency and standard for interoperable digital radio networks got off to a good start. After an initial (and more general) congressional mandate in 1983,[16] the FCC issued a first "Report and Order" in 1987 envisioning intercommunication channels as part

[15] The PSWN report "Comparison of Conventional and Trunked Systems" (May 1999), for example, concludes that "[t]ypically trunking allows a system to serve more users with the same amount of spectrum or less. Since spectrum has become a scare resource, this property of trunking will drive its use in the future" (p. 46)

[16] Federal Communications Commission Authorization Act 1983, Pub. L. No. 98-214, § 9(a), 97 Stat. 1467 (1983).

of a national plan for public safety agencies.[17] In 1993, as part of the Omnibus Budget Reconciliation Act, Congress asked the FCC to develop a framework to ensure that public safety communications needs are met through the year 2010. Interoperability was included in the request as a primary objective of this new framework.[18] The FCC was uniquely positioned to provide such a framework, as it not only maintains jurisdiction over the use of radio spectrum, but may also condition spectrum use.

Unfortunately, the FCC approached the subject like any other spectrum allocation matter. Expending valuable time, it first studied the issue for two years and set up an advisory committee (the Public Safety Wireless Advisory Committee, or PSWAC).[19] It soon became clear to the FCC that it faced numerous powerful stakeholders in its efforts to fulfill the congressional mandate.

The FCC's first task was to identify a portion of the radio spectrum that could be used nationwide by public safety organizations. This was difficult, as it required clearing spectrum from existing users, most of which had not only substantial investments, but also valid legal claims to use, these frequency bands. Fortunately, the FCC was already negotiating with television stations their planned transition from analog to digital television (DTV). DTV transmits more information than analog television, and thus requires a frequency band higher up in the radio spectrum than those currently in use for terrestrial transmissions of TV signals. In their shift toward a new portion of the radio spectrum that can accommodate DTV, TV network operators are vacating the radio spectrum they have used for analog TV. A part of this spectrum, once vacated, may be rededicated for interoperable public safety radio networks.

---

[17] See Report and Order, 3 FCC Rcd 905; as well as the more daring Notice of Proposed Rule Making, 2 FCC Rcd 2869 (1987).

[18] See 47 U.S.C. § 309(j)(10)(B)(iv) as added by Pub. L. No. 103-66 (1993); note that the congressional mandate was to provide a framework for public *safety* communications, which involves a narrower group than public *service* organizations. The FCC later redefined "interoperability" to encompass the wider definition of providing "an 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" "Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Agency Communications Requirements Through the Year 2010", WT Docket No. 96-86, First Report and Order and Third Notice of Proposed Rulemaking, 14 FCC Rcd 152, 189–90 ¶ 76 (1998).

[19] Pursuant to the Federal Advisory Committee Act, 5 U.S.C. App. 2 (1988).

After prolonged deliberation, in 1997, the FCC issued its order, allocating 24 MHz of vacated spectrum in the 700 MHz band to public safety services.[20] It also stated that it would initiate separate proceedings to set the conditions for use of this portion of the spectrum.[21] As part of these proceedings, the FCC issued its important First Report and Order and Third Notice of Proposed Rule Making, specifying use and service rules for this spectrum, in summer of 1998.[22] It appeared as though, five years after Congress mandated action, the FCC had finally embarked upon a specific plan to enable interoperability. It had identified a common frequency spectrum and initiated proceedings to define "service rules" for its use, providing the necessary groundwork for a common technical standard. But this apparently bright picture is darkened by some important caveats.

First, television broadcast stations have until December 31, 2006, to move from analog to digital broadcasting. Hence only in 2007, fourteen years after the initial congressional mandate was issued, will public safety organizations in the United States have spectrum available nationwide for interoperable communication. It almost seems as if the FCC misunderstood the congressional call to ensure that public safety communications needs were met *through* the year 2010, and instead aimed by meet them *by* the year 2010. Granted, the situation is not as bleak in reality as it looks on paper. In many areas of the United States, television broadcasters are not using channels 60–69—the spectrum in question—and public safety organizations can utilize such unused spectrum right away. In many urban and suburban areas, however—exactly where public safety organizations have to communicate most frequently—these channels are in use. Moreover, until September 2001 the FCC required television broadcasters wanting to move out of channels 60-69 to switch immediately to digital broadcasts. Given the minuscule number of digital receivers in use and the resulting smaller viewer base for such broadcasts, television stations had no incentive to vacate the spectrum earlier than the end of 2006. Recently, the FCC has mitigated this situation by issuing an order permitting

[20] See "Reallocation of Television Channels 60–69, the 746–806 MHz Band", ET Docket No. 97–157, Report and Order, 12 FCC Rcd 22953 (1997).

[21] Ibid.; see also "Advanced Television Systems and Their Impact Upon the Existing Television Broadcast Service", MM Docket No. 87-268, Sixth Further Notice of Proposed Rule Making, 11 FCC Rcd 10968–10980 (1996).

[22] "The Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Agency Communications Requirements Through the Year 2010", WT Docket No. 96-86, First Report and Order and Third Notice of Proposed Rulemaking, 14 FCC Rcd 152 (1998).

broadcasters to migrate to available spectrum for analog broadcasts and switch to digital broadcasts only in 2007—a positive move.[23] But another three important years were lost in the process.

Second, whereas the FCC has looked (too) far into the future when selecting a frequency band, its ventures into defining the communications standard have been fundamentally retrospective. Very early in the process of defining an appropriate technology, the commission understood the implications of large-scale interoperability within a limited portion of radio spectrum. As a result, it leaned toward trunked digital networks utilizing advanced compression of voice and data to accommodate as many interoperable channels as possible in the available 24 MHz. This was as prudent a move as it was obvious, given the advancements in technology and the requirements of interoperability.

At the same time, the FCC realized that interoperability depends not only on defining a framework, but also on stakeholder buy-in. With tens of thousands of stakeholder organizations (some of which wield substantial power) on the local, state, and national levels, the FCC wanted to involve as many stakeholders as possible in the deliberations over rules and standards. This was not a novel situation for the FCC. In fact, the FCC's traditional deliberative process is designed to integrate stakeholder views. By also applying this process to the area of public safety communications, the FCC hoped to create a positive momentum furthering the acceptance of its envisioned framework.

Like the FCC, the stakeholders saw a need for interoperability, but for them interoperability had to be balanced against a number of other needs and constraints. All public safety organizations, through their various national associations, expressed concern about the cost of a national interoperable network as envisioned by the FCC.[24] In addition, many of the local and state public safety organizations feared being marginalized by large, powerful federal agencies eloquently taking positions. The formation of the Public Safety Wireless Network (PSWN) program as a joint initiative of

[23] Action by the Commission September 7, 2001, by Order on Reconsideration of the Third Report and Order (FCC 01-258).

[24] For example, in its reply to the FCC, the Association of Public Safety Communications Officials International (APCO) stated that "[t]here are legitimate technical, operational, and feasibility reasons why some local governments must maintain conventional systems"; see Reply A96-86, available online at http://www.apcointl.org/gov/a96-86.doc.

the Departments of Justice and the Treasury advocating interoperability did not help to alleviate their misgivings. Despite PSWN being targeted at state and local public safety agencies, many of these agencies remained suspicious of federal involvement in what they perceived was largely a local or regional issue. By the same token, federal agencies were convinced that a substantial technological step forward was necessary, especially in the wake of interoperability breakdowns like those that occurred during the response to the 1993 World Trade Center and 1995 Oklahoma City bombings. Realizing the resistance of local agencies only prompted them to push harder for an advanced solution.

The struggle was exacerbated by the fact that a number of public safety stakeholders, acutely aware of some of the technical shortcomings of their analog systems, had already engaged in years of deliberation over a potential new communications standard. The core of the standard they envisioned, however, was not just interoperability, but also limited backward compatibility. Moreover, they were wary of replacing existing networks with new hardware given their budgetary restraints. Their focus, therefore, was on small, evolutionary steps toward a more modern communications infrastructure. To that end, they had teamed up with the Telecommunications Industry Association (TIA) and the Electronic Industries Alliance (EIA). In addition, Motorola, a major vendor of radio communications equipment, became heavily involved in the process. The aim was to define a standard that would expand the capabilities of the communications networks and introduce some interoperability, but also to extend the life of analog networks. The resulting initiative, called Project 25, ultimately yielded a set of ANSI(American National Standards Institute)/TIA/EIA standards for communications networks. Its aim was to convince the FCC to require users of the 700 MHz band to use Project 25–compliant equipment.

The Project 25–based standard[25] differs in two fundamental ways from what the FCC had originally envisioned.[26] First, although it permits trunked networks, it does not *require* networks to be trunked, limiting the potential efficiency gains associated with trunking. It also features a less sophisticated compression technology than that envisioned by the FCC, using 12.5 KHz of spectrum

[25] I am referring here to a Project 25-based "standard", although it actually is a bundle of complementary standards. Yet, for reasons of brevity and readability I will refer to it in the singular.

[26] See "Project 25 Standards Explanation, February 2001", available online at http://www.motorola.com/publicsafety/docs/P25_white_paper.doc.

for each voice channel and not just 6.25 KHz as the FCC originally hoped[27]. Hence, only half as many channels are available in a given spectrum, and with no trunking requirement, even these will not be managed to maximum efficiency. Second, the FCC had hoped for a vibrant market of hardware providers for the required radio network equipment. After all, more than $18 billion of investment was at stake in the United States alone. Yet by 2000 only one major vendor, Motorola, had released networking equipment capable of providing a Project 25–compliant trunked digital network,[28] and only a handful of smaller vendors offered equipment for less powerful, nontrunked networks. This ran counter to the FCC's idea of intense vendor competition promoted by open standards promoted. How could public safety organizations ensure that they received value for their money when a single vendor effectively dominated the market?

For some, the FCC did not go far enough. But for many public safety organizations involved, it went dangerously far. They saw interoperability as one of the many challenges they faced and estimated that the likelihood that they would have to confront a catastrophic event requiring comprehensive interoperability was slim. Their aim was to get the FCC to water down any strong interoperability requirements and thereby to minimize any potential impact on their budgets.

Cognizant of how the stakeholders' lined up on the issue, the FCC tentatively opted for requiring public safety organizations using the 700 MHz band to use Project 25–compliant, trunked digital networks, proposing essentially a compromise between Project 25 and its own higher aspirations. Insisting that the networks be trunked, and suggesting what it termed a "migration path" toward a better compression technology using only 6.25 kHz of spectrum, the FCC had apparently hoped to maintain its ultimate goal by pushing it farther into the future.

Stakeholders' reaction to the FCC's tentative requirements was mostly negative. Many public safety organizations feared the financial consequences of such a mandate and pressured their national associations to lobby against it. Furthermore, they argued that oversight of interoperability should be performed at state level, hoping to be more effective lobbyists there. When a group came

[27] See First Report and Order, 14 FCC Rcd at 205 ¶ 113.

[28] See http://www.motorola.com/publicsafety/70-10.shtml.

forward advocating that the FCC adopt a much more sophisticated standard[29] called TETRA (Trans European Trunked Radio networks), which had already proven its operability in Europe, the Project 25 Steering Committee immediately sensed the danger of a strong competitor. Understanding that it had more to fear from TETRA than from reluctant public safety organizations, it decisively shifted its strategy. In tune with many public safety organizations, the committee started to downplay the need for comprehensive interoperability and began to argue that a limited number of interoperability channels, managed either through a trunked network infrastructure or even just manually, as in the old days of analog radio, would be sufficient for almost all emergency situations. At the same time, it began to emphasize potential disadvantages of trunked systems and to extoll the virtues of a more gradual approach of including all stakeholders and providing backward capabilities. Finally, in a brilliant strategy of containment, Project 25 proponents set up an industry working group with some TETRA proponents to begin discussions about the possibility of an eventual second-generation common standard.[30]

Few insiders were shocked when the FCC, in its Fourth Report and Order and Fifth Notice of Proposed Rule Making published in January 2001,[31] effectively rescinded its initial stance of comprehensive interoperability. A limited version of the Project 25 Standard (termed "Phase I") was adopted, based on the less efficient 12.5 kHz channels. The original mandate for trunking was replaced by almost the opposite: a prohibition of trunking except in 8 of the available 128 channels[32] originally allocated for narrow-band interoperability. And a possible migration path to a more spectrum-efficient compression technology was put on the back burner and subjected to "further study."

---

[29] Similar to the Project 25 "standard", the TETRA "standard" is a bundle of many complementary standards. For reasons of brevity, however, I will refer to it in the singular.

[30] There is also a less cynical interpretation of the formation of this working group: a sincere desire to bridge the technological divide and create true global interoperability, especially after the events of September 11; see "Transatlantic Public Safety Partners meet in the wake of U.S. Terrorist Attacks", ETSI/TIA/Project Mesa press release (September 24, 2001); see also "New Transatlantic Partnership Addresses Mobile Broadband Specifications for Public Safety Applications" (October 20, 2001).

[31] Fourth Report and Order and Fifth Notice of Proposed Rule Making, WT-Docket No. 96–86.

[32] See the Third Memorandum Opinion and Order and Third Report and Order, 15 FCC Rcd at 19851–19860 ¶¶ 16–39.

Almost a decade has passed since the FCC ventured into developing a framework for interoperable communications among public safety organizations. Despite its understanding of the issues and its good intentions to involve the important stakeholders in the development process, the results have been dramatically misaligned with the needs of the present. Selecting a frequency band that would be fully available only at the beginning of 2007 for use by public safety organizations, the Commission looked far into the future, while at the same time selecting a technological standard wedded to a predigital, preinformation age. Therefore, despite all of the activities of an entire decade, substantial parts of the second hurdle remain in place.

(c) Funding: Concerns

The difficulties of establishing a common frequency and standard pale compared with finding funding for an advanced, interoperable public safety communications network. The situation is easy to describe and difficult to rectify. Most public safety agencies are acutely aware that their communications networks are outdated and need to be replaced, especially if the goal is comprehensive interoperability. Many plan to replace their equipment, but the overwhelming majority cannot find the funding to do so and do not expect to be able to in the near future. This dismal outlook is in line with studies estimating the total amount of investment needed, as well as the monies available now and in the foreseeable future through public (federal, state, and local) and private sources. Funding appears to be the final and most formidable hurdle on the road to interoperability.

There are almost 60,000 individual public safety organizations in the United States comprising more than 2.2 million personnel.[33] Thirty-seven percent of these organizations are (currently) planning to replace their aging radio systems with new equipment.[34] Forty percent of all fire and EMS agencies plan to switch to a trunked digital system,[35] and numbers for state and local law enforcement agencies' procurement plans are similar.[36] These agencies seem to have a good sense of the

[33] PSWN, *A Priority Investment for America's Future Safety*, p. 5.

[34] Ibid., p. 4.

[35] PSWN, *Analysis of Fire and EMS Communications Interoperability*, p. 9.

[36] National Institute of Justice, *State and Local Law Enforcement Wireless Communications and Interoperability* (January 1998), p. 1.

broad technological trends. Their individual procurement plans are well aligned with the general goal of increased interoperability. The problem is securing the necessary funding for the investments they have planned. Agencies recognize the difficulty of the task of obtaining this funding. Sixty-nine percent of all law enforcement[37] and sixty-eight percent of fire and EMS agencies[38] recently stated that lack of funding was a severe obstacle on their path to interoperability.

Moreover, these are not just the subjective impressions of agencies that will have to make—and fund—the necessary upgrades. Independent studies have verified the need for tremendous amounts of funding to finance the necessary network upgrades for interoperability. One such study, undertaken by management consulting firm Booz-Allen & Hamilton on behalf of PSWN, estimated a total capital need of $18.3 billion to replace the existing communications infrastructure. Importantly, the costs to be borne by local agencies account for more than 80 percent of that amount ($15.4 billion), compared with $1.2 billion for federal and $1.7 billion for state agencies.[39] This implies that the organizations most burdened with finding sufficient funding are precisely the ones that have no direct access to larger federal or state budgets.

In addition, the amount of funding needed involves more than just the cost of replacing equipment. Provision also has to be made for planning, procurement, training and maintenance costs over the entire life cycle of the new systems.[40] In fiscal 2000 the White House sought, but Congress denied a budget request for $80 million in "seed" money available to states to plan statewide public safety wireless communications systems and create demonstration projects.[41] Even if these public funds had been available (and the only federal funds for that purpose), it would have taken a staggering 225 years of funding at that level to replace the public safety radio networks nationwide.

---

[37] Ibid, p. 8.

[38] PSWN, *Analysis of Fire and EMS Communications Interoperability*.

[39] PSWN, *LMR Replacement Cost Study Report*, p. 4

[40] See Booz-Allen & Hamilton, *Report on Funding Strategy for Public Safety Radio Communications* (October 1998), p. ii.

[41] This severe shortfall was in direct opposition to the recommendations made by the Interagency Working Group on Funding (IWGF), and was covered in the PSWN, *Report Card on Funding Mechanisms*, p. ES-3 (last bullet point), 8 (section 3.2.1), 17 (recommendation 1). The original report by the IWGF in June 1998, p. 23–26 recommended federal funding that would have totaled $162 million over 4 years, but was never appropriated.

Fortunately, there are other financial sources available on federal, state, and local levels to assist in funding communications network upgrades.[42] For instance, under the Community Oriented Policing Services–Making Officer Redeployment Effective Grants (COPS-MORE), up to $81 million in federal funding was available in 2001 to law enforcement agencies for the purchase of information technology equipment.[43] The Edward Byrne Memorial State and Local Law Enforcement Assistance program provides $63 million in discretionary federal funds.[44] Other federal funding sources include FEMA,[45] Local Law Enforcement Block (LLEBG),[46] National Telecommunications and Information Administration (NTIA),[47] and State and Community Highway Safety grants as well as the forfeiture funds of the Department of Justice[48] and of the Treasury.[49]

As good as this sounds, these funding sources have a number of disadvantages that are cumulatively quite discouraging. Most of the discretionary funds are heavily earmarked for very specific aspects or contexts (thus limiting their utility to fund interoperable communications systems), and many of the grant programs require matching funds from the agency applying for grants—from 25 to 50 percent of the total amount requested.[50] As local agencies have to reconcile buying into a new radio infrastructure with many other budgetary demands, matching even the 25 percent threshold may be difficult for them. Consequently, these federal grants may end up being accessible primarily to agencies that have already lined up significant seed funding of their own. Moreover, many of

---

[42] See PSWN, *The Report Card on Funding Mechanisms for Public Safety Radio Communications* (August 2001), and Booz-Allen & Hamilton, *Report on Funding Mechanisms for Public Safety Radio Communications* (December 1997).

[43] U.S. Department of Justice, COPS MORE Fact Sheet (Washington, D.C.) (May 2001).

[44] PSWN, *Report Card*, p. 20.

[45] The total amount of FEMA grants in 2000 was $137 million, with $2.4 million the size of the average grant. Grant monies awarded by FEMA have to "improve and maintain state and local capabilities for addressing all hazards".

[46] $523 million was provided in FY00 and FY01 for this grant program.

[47] In FY00 a total of $15.5 million was awarded by the NTIA, with the average amount per recipient being slightly over USD 400,000.

[48] Information on the Department of Justice Assets Forfeiture Fund is available online at http://www.usdoj.gov/jmd/afp/06fund/indextxt.html

[49] Information on the Department of the Treasury Forfeiture Fund is available online at http://www.ncjrs.org/htm/tff.htm

[50] PSWN, *Report Card*, p. 19–21.

these funding sources are limited to specific parts of the system life cycle, like procurement, and do not cover other stages of the cycle, like planning or training.[51]

On the state level, the most promising funding source is an FCC-mandated surcharge levied on cellular phone operators for wireless 911 services. In accordance with the FCC mandate, states have to use the income from the surcharge to improve 911 response capabilities. For example, for the state of Iowa, this surcharge generated quarterly revenues of more than $1 million in 2000 to enable the state to meet FCC emergency calling regulations.[52] Once the state has complied with the initial FCC mandate to improve 911 capabilities, income from the surcharge may provide a more direct funding source for public safety communications. State budget appropriations, state grants, state targeted taxes, and state bond issues[53] may provide additional sources of funding. Similar local funding is possible as well, although its size is generally limited.

But none of these sources is targeted specifically at funding modern, interoperable radio communications networks. Being much more general in nature, they provide no incentives for agencies to choose specifically an interoperable system. Given the limited amounts of funding available, the requirements for matching funds, and the fact that agencies have legacy communications systems in place, there is a real danger that most funds obtained through these sources are going to be used to maintain and step up existing systems, not replace them. The funding mechanisms mirror and reinforce the crippling "small-steps" approach already permeating the frequency and standard-setting debates.

More unorthodox ideas, such as the sharing of systems among agencies and the promotion of partnerships with other public- and even private sector-actors, like utility companies, have been suggested and with some success implemented in individual cases.[54] Yet for most public safety

---

[51] This problem is detailed in PSWN, *Report Card*, p. 7–16.

[52] Ibid, p. 23.

[53] According to the PSWN, *Report Card*, p. 27, the Commonwealth of Massachusetts successfully used a bond issue to construct a statewide 800-MHz radio communication system using trunking technology.

[54] See for example the "Hamilton County Digital Communication Network," available online at http://www.mobilecomms-technology.com/projects

agencies in the United States, moving to a new digital and interoperable communications network is still synonymous with planning, procuring, and maintaining a new infrastructure funded through a traditional mix of local, state, and federal sources. With limited funds available, such a strategy faces huge obstacles, pushing the ultimate goal of comprehensive interoperability far into the future.

As established above, three hurdles have to be overcome to achieve interoperability: technology, common frequency and standards, and funding. As we have seen, the appropriate technologies to enable interoperability are available. In addition, steps have been taken to designate a common frequency and set a common standard for the systems. With a common, nationwide frequency band not available before 2007, however, and the selection of an outdated standard, these steps hardly provide interoperability in the short to medium-term. Moreover, the limited funding available and how that funding is targeted make it very difficult for agencies to overcome the third hurdle. Unsurprisingly, agencies have looked elsewhere for pragmatic alternatives to mitigate the interoperability crisis.

(d) Pragmatic Alternatives—and their Pitfalls

The focus of this paper thus far has been on achieving interoperability by creating a comprehensive digital network. In such a network, communication across agency lines happens seamlessly. Yet this is not the only way interoperability can be accomplished. Neither is interoperability a novel concern. Since the early days of radio communication, agencies have had a need to integrate operations. Over time, they have developed a variety of "low-tech" methods to work around communications incompatibilities, like posting representatives in dispatch centers to relay information and issuing mobile radios to other agencies.[55]

Such pragmatic solutions will work for many routine situations. But what catastrophes like the Columbine High School shootings and the Oklahoma City and World Trade Center bombings demonstrate is the need to have interoperability work not just in routine operations, but in extreme situa-

[55] See Mary J. Taylor, Robert C. Epper, and Thomas K. Tolman, "Wireless Communications and Interoperability Among State and Local Law Enforcement Agencies" (Research Brief, National Institute of Justice, January 1998), p. 8.

tions with hundreds of first responders from different agencies and locations. Simple low-tech methods cannot provide this level of interoperability.

There is another way, though, to provide "thicker" interoperability while utilizing the existing communications systems. Together with vendors, FEMA and other agencies have developed special equipment, so-called cross-band switches, to patch together two existing incompatible communications networks.[56] In simple terms, two radios are connected via these switches so that everything received by one radio is automatically retransmitted by the other, and viceversa, creating the illusion of one interoperable network. FEMA has outfitted a number of trucks with this equipment, keeping them ready for deployment at its regional offices. Many other agencies, also facing interoperability challenges, have installed such equipment.[57]

This solution has a number of advantages. It is far superior to low-tech methods as communication seems to flow freely between incompatible networks. Sophisticated Multi-Radio Vehicles (MRV) in use by FEMA can link a multitude of communication networks if necessary[58] to provide an almost seamless communication experience among different networks and across incompatible frequencies. Unlike in "deep" interoperability, no new hardware is needed to implement this type of "shallow" interoperability apart from the equipment linking the networks, which saves resources compared to the costs of a full conversion. Users can retain their radios, and agencies can still operate their conventional networks. Even new digital networks can thus be incorporated step by step and connected to existing analog networks. No common frequencies are needed, and no new standards must be set. The equipment is ready today, and deployment is comparatively simple and straightforward.

Originally intended more as a stopgap measure until the realization of a nationwide comprehensive interoperable network, this pragmatic solution has gained substantial momentum. At the

[56] For example, the ACU-1000 Intelligent Interconnect System by JPS Communications.

[57] Roman W. Kaluta, "New Developments in Interjurisdictional Communication Technology" (January 2001), available online at http://www.iacptechnology.org/TechTalk/TechTalk0401.htm; see also "AGILE: Research, Development, Testing and Evaluation of Interoperability Technologies," available online at http://www.agileprogram.org/research.html.

[58] See http://www.fema.gov/r-n-r/mers04.htm.

same time, there are obvious downsides to network patching. Multiradio equipment can link only those networks the frequency and standards of which it supports. The greater the number of networks to be linked, the more complex and expensive the equipment necessary to link them. Linking may "create" one network, but it does not permit this network to be divided into subgroups. This in turn limits the ability of the network to accommodate a large number of users, making it difficult if not impossible to create interoperability on all levels of command. The technique uses existing radio networks with potentially poor reception and voice transmission quality. It is largely limited to voice; interconnecting data streams or other added services like conference calling, faxing, or calling gateways is difficult to implement, as is providing for encryption of communication. Moreover, interoperability is happening on a network level, not on the level of individual users. For example, when their network collapses, firefighters will be unable to use their radios with the police radio network. Also, emergencies may occur where there is no multiradio equipment in place. Although FEMA has mobile units stationed around the country, it takes some time to get them on location and working. This will preclude interoperability in the hours immediately after an emergency, arguably the time interoperability is in highest demand. In sum, multiradio equipment has severe limitations as a tool for interoperability. Fundamentally, it is little more than a patch until networks are deployed that provide comprehensive interoperability on the user level.

Yet there is an even deeper danger: Cash-stripped public safety agencies may decide to substitute plans for advanced interoperable networks with multiradio equipment, thinking that one is about as good as the other. There is already a trend toward doing this, and the potential consequences are dramatic. If this trend continues, tens of thousands of public safety agencies in the United States will exit the first decade of the new millennium with the same equipment that proved insufficient at major emergencies twenty years earlier. Despite a head start in realizing the problem, the nation will have drawn out its interoperability crisis, and will have long been overtaken by many other nations in terms of achieving interoperability.

Comprehensive interoperability is still an elusive concept in the United States. The hurdles that must be cleared to achieve it have been well identified, but the strategies to overcome them have—at least so far—shown limited tangible results. One might argue that this is a general problem of interoperability, not one specific to the United States. But other nations have successfully mastered the challenge under even less fortunate circumstances. The following section analyzes how the

Europeans have approached interoperability. Starting at about the same time as the United States did, yet handicapped by even more complicated political structures than those in the United States, the Europeans surprisingly have tackled the interoperability hurdles more forcefully, and so far more successfully, than their colleagues in the United States.

III. European Interoperability: Succeeding against the Odds

Galtuer[59] is an idyllic little village in the Austrian Alps, 5,250 feet high, at the end of a long valley on Tyrol's southwesterly border; it is also a leading ski resort. By the end of the 1990s, 3,000 beds in hotels and inns, run by its 700 inhabitants, accommodated thousands of tourists from around the globe.

The winter of 1998–99 produced one of the heaviest snowfalls in recent history. At the end of January 1999, it started to snow and hardly stopped for the next four weeks. By the second week of February, Galtuer was snowed in, the threat of avalanches making its only road downhill impassable. But most tourists in Galtuer hardly noticed. Their hosts, used to extreme winters, had stocked up on necessities.[60] To keep the tourists happy the tourist office had even organized a tobogganing race at the town square on Tuesday, February 23.[61] A week earlier, the road had become usable again for a few days, and a new horde of skiers had come to the village.

Shortly after 4 pm on February 23, three gigantic avalanches slammed down the steep mountain slope, advancing right into town. The snow was heavy, "like concrete," eyewitnesses later commented. It buried sixty people. Within minutes hundreds of people began searching for those who were trapped under the snow. Thirty-one people died that day in Galtuer, and scores more were

[59] The following description is based on press reports as well as interviews conducted in November 2001 by the author, including two interviews with Werner Senn.

[60] "Schnee", *Der Standard*, February 11, 1999.

[61] "Lawinenkatastrophe - Galtür: Die Lawine platzte mitten in ein Urlauberrennen," *Der Standard*, February 27, 1999.

wounded.[62] Yet this was only the beginning. Snowfall made it impossible for rescuers to reach Galtuer by helicopter that day.[63] The road, still closed because of the snowfall, offered no alternative.

The avalanche had also cut the only power line. But Galtuer had diesel aggregates that provided sufficient electricity for all essential activities. And cellular phone relay stations, though quickly overloaded, seemed to work even hours after the power was cut. On Wednesday morning, the weather was good enough for helicopters to rescue the wounded and to deliver food and fuel. Hope was growing in Galtuer. But by early afternoon, the weather had once again deteriorated. Shortly thereafter, another avalanche hit houses outside the village, burying another nine people.[64] Cellular phones stopped working as the batteries in the relay stations, still without power, ran out of juice. More than 12,000 tourists were trapped in Galtuer. The town's only remaining connection to the world was a one-channel analog radio link of the Austrian gendarmerie.

From his command post in Landeck, some thirty miles away, Werner Senn, assigned by the Ministry of the Interior to coordinate the Alpine gendarmes in the area, started organizing the rescue mission minutes after the first avalanches had hit Galtuer. Fortunately, the weather improved. Alpine gendarmes were flown into the village and the outlying hamlets to establish radio links. Over the next couple of days, the gendarmes' lone analog radio channel provided the communication infrastructure for a massive evacuation effort. With the help of fifty-two helicopters from Austria, Germany, France, and the United States, more than 12,500 tourists were flown out of Galtuer and environs. To communicate with one another, they too, were equipped with the old radios of the Alpine gendarmerie. The true miracle of Galtuer, Senn recalls, was that in over 1,500 sorties flown through a tight, V-shaped valley, with poor visibility and frequent snowfall, directed only by a single crackling analog radio link, more than 17,500 people were transported without a single accident.

For Europe, the drama of Galtuer was tantamount to that of Columbine High in that it exemplified the interoperability crisis and restated the need to get it fixed. Through low-tech methods of deploying radios of the only working network to everyone involved, the rescuers of Galtuer could

---

[62] :Nach Lawine 55 Menschen vermisst," *Der Standard*, February 24, 1999.

[63] "'Es war einfach unmöglich': Warum Hubschrauber nicht fliegen konnten," *Die Presse*, February 25,1999.

[64] "Zweite Lawine krachte ins Tal: Suchhund rettete vierjähriges Kind," *Die Presse*, February 25, 1999.

coordinate better, Senn maintains, than if each team of responders had used its own network. The forced interoperability had its advantages. It made everyone remain focused and informed. But the shortcomings of this setup were all too evident. Helicopter pilots shuttling tourists out of the steep valley could hardly make use of the radio. Despite everyone's trying to speak only when absolutely necessary, the channel quickly became overloaded. Rescuers wondered how long the old crackling network would last. Had that one available communications link broken down, Galtuer might have turned into a catastrophe. Not just for the hundreds of first responders involved in Galtuer did the need to have an interoperable system, and with *more than one* channel, became painfully obvious.

In Europe, the debate over interoperable radio communication networks emerged at about the same time as it did in the United States. But the process necessary to make interoperability a reality faced structural hurdles in Europe that were not present in the United States. Unlike the United States, the European Union is not a federal state. Individual member nations retain substantial decision-making power, making coordination among them more difficult. In addition, Europe's high-tech industry traditionally has lagged behind its American counterparts. For decades, national regulatory bodies, not European-wide agencies enacted frequency plans, splintering the radio spectrum geographically. And the European Union was not in a position to help much either. Radio networks for public safety agencies were associated with law enforcement, a policy area originally excluded from EU decision making. Some European nations had agreed on cross-border law enforcement cooperation, but these agreement were developed outside of the European Union structures. Finally, the severe constraints imposed on EU members' national budgets since the mid-1990s by the so-called Maastricht criteria shattered any hope for the spending flexibility needed to fund an interoperable radio network.

Still, Europe quickly overtook the United States in the march towards interoperability, partly through ingenuity and a can-do attitude, and partly because of sheer luck. Today it is well on its way toward an integrated continent-wide public safety radio communications network providing comprehensive interoperability on all levels.

(a) Technology: Picking a Winner

Planning for a mobile digital trunked radio system (MDTRS) to be used by both the public and private sectors in Europe started in the late 1980s. MDTRS later evolved into a technology called TETRA[65]. TETRA is a trunked digital system permitting voice and data transmissions.[66] One of its strengths is its ability to scale, from a few dozen to hundreds of thousands of users across an entire continent.

TETRA technology offers comprehensive interoperability. Not only can TETRA-compatible *networks* easily be linked together: Interoperability is implemented all the way to the level of individual radio *handsets*, enabling users from one TETRA network to use their handsets within the infrastructure of another TETRA network. Interoperability in TETRA is software enhanced, permitting dispatchers to set up talk groups in advance, for example, among the commanders of various public safety agencies, as well as to create talk groups on the fly, generating communication links for task forces and emergency teams formed ad hoc.

Because of Europe's congested radio spectrum, spectrum efficiency plays a prominent role in TETRA. A sophisticated voice compression system, with voice channels taking up only 6.25 kHhz of bandwidth, allows TETRA to bundle four such channels into a 25 kHz band—and not just two as with U.S. Project 25 technology.[67] As a Time Division Multiple Access (TDMA) trunked system, TETRA technology automatically manages channel allocation to maximize spectrum efficiency.[68]

Prioritization is an additional capacity TETRA offers. All requests for communication are queued and allocated based on level of priority, which is pre-selected for each radio handset. This

---

[65] See the discussion of the development of the Project 25 standard, *supra*.

[66] For a description on how the TETRA standard was developed, see section III (b).

[67] See Tony Kent, "Understanding TETRA Voice Coding," available online at http://www.tetramou.com/Presentations/IIR/Codec.zip.

[68] As noted above, one of the disadvantages of trunked systems is the coordination overhead required to set up a communication link. Because of optimization, TETRA is able to complete such a setup within 300 ms of the time the request is made by a user.

permits commanding officers to get preferred access in times of congestion. Emergency priorities afford users with an immediate talk line, even if all channels are in use. And unlike conventional analog radio networks, TETRA incorporates a number of security features, from handset authentication[69] to optional two-way encryption.[70] Through multiple gateways, TETRA users are connected with other telecommunication networks and can place phone calls or make TCP/IP (Internet) requests.[71]

Second-generation TETRA technology, in use since the late 1990s, overcomes the primary Achilles heel of trunked radio systems: the need for a trunked infrastructure. In what is called "Direct Mode",[72] TETRA users may talk with each other directly, even if they are out of reach of a network infrastructure (for example inside a building or in a steep valley). Basic communications services are available in Direct Mode, including communication prioritization for emergencies. Any second-generation TETRA handset can also act as a small relay station connecting Direct Mode users to the trunked network infrastructure, thus in effect expanding network reach.

By 2000, more than a dozen large telecom corporations had commenced producing a wide variety of equipment—both network infrastructure and handsets—based on the TETRA technology, including Finnish cellular phone leader Nokia, British telecom provider Marconi, defense contractor Matra, Canadian telecom giant Nortel, and, perhaps most surprisingly, given its support for Project 25 in the United States, Motorola.[73] Despite initial U.S. technology leadership in this area, Europe leapt the first hurdle toward interoperability in stride.

---

[69] Such authentication enables the network to check whether a particular radio handset is "permitted" to take part in a specific (group) call, even if the handset is from outside the local network.

[70] Gert Roelofson, "Introduction to TETRA Security," available online at http://www.tetramou.com/files/Tetrasec.doc; Peter Wickson, "TETRA Security," available online at http://www.tetramou.com/Presentations/IIR/SecuritySIM.ppt.

[71] Mehdi Nouri, "TETRA Standard Interfaces and Gateways," available online at http://www.tetramou.com/files/Mehdi%203.doc; Mehdi Nouri, "TETRA Standard Interfaces," available online at http://www.tetramou.com/Presentations/IIR/Interfaces.ppt.

[72] For a description of "Direct Mode" see Ranko Pinter, "TETRA Direct Mode," available online at http://www.tetramou.com/files/TETRADMO.rtf.

[73] See Pekka Blomberg, *TETRA: State-of-the-Art Global PMR Standard* (1999); see also the Tetra Memorandum of Understanding website at http://www.tetramou.com. Motorola markets its TETRA-compliant systems under the name of DIMETRA; see Motorola, "TETRA System Architecture," publication L0592 GBV 5 98-0.

(b) Frequency and Standards: Working in Tandem

Early discussions concerning a common, European-wide frequency for public safety communications did not start within the context of the European Union, but within the Schengen group, a framework for enhanced cross-border coordination and cooperation of law enforcement agencies. In 1991, the Telecom working group of the Schengen framework contacted the European Radiocommunications Committee (ERC), which coordinates the use of radio spectrum in Europe to "identify some harmonised spectrum for exclusive use by the police and security services across Europe."[74] ERC then negotiated with NATO to release initially 6 MHz, and later 10 MHz, of spectrum previously reserved for NATO use for such purposes.[75]

By 1993, the use of a harmonized spectrum had been broadened from law enforcement to all emergency services. The Schengen framework had been incorporated into the European Union's "third pillar,"[76] anchoring interoperability squarely within EU competency. At the same time, the European Telecommunications Standards Institute (ETSI)[77] initiated a fast-paced process for developing a TETRA standard for voice and data communications. Unlike the slow-moving inclusive process in the United States, ETSI proceeded swiftly. By 2000, more than 300 documents related to the TETRA standard had been published.[78]

Aware of ETSI's work, the Schengen group agreed upon a common communications specification and subsequently asked ETSI whether ETSI had a standard that met its specification.[79] ETSI replied that one of its standards, TETRA, did fulfill the specification. Although the European Union

[74] ERC, "Harmonisation of Frequencies for Police and Security Services in Europe".

[75] See also ERC, Harmonised Radio Frequency Channel Arrangements for Emergency Services Operating in the Band 380–400 MHz, Recommendation T/R 02-02 E (1993, revised 1997).

[76] Treaty on European Union, articles 29–42, Official Journal C 340, 10.11.1997, pp. 145–172.

[77] See http://portal.etsi.org/directives/home.asp.

[78] These documents are available for download at http://www.etsi.org.

[79] "ERC Decision of 7 March 1996 on the harmonised frequency band to be designated for the introduction of the Digital Land Mobile System for the Emergency Services" (ERC/DEC/(96)01).

Police Co-ordination Council, which replaced the Schengen group when the Schengen framework was incorporated into the European Union, retained final decision power over the standard to be chosen for a European-wider interoperable communications system for public safety organizations, the choice for TETRA was a foregone conclusion.

In 1996, the ERC designated 10 MHz in the 380–400 MHz band for digital land mobile systems of emergency services.[80] A 6 MHz band was to be made available by 1998, with the remaining 4 MHz to follow shortly thereafter. Only systems compliant with ETSI standards were permitted to be used, in effect restricting of the 10-MHz use to TETRA-compliant hardware.[81] Unlike FCC mandates, ERC decisions are not automatically binding. European member states need to decide to implement ERC plans. And they did: By 2001, twenty-six European nations had set aside the frequency bands designated in the ERC decision.[82]

Only four European nations refused to accept the common TETRA frequency and standard: France, Sweden, the Czech Republic, and Slovakia. Repeating telecommunications history, France, which decades earlier had selected an incompatible television standard called SECAM while the rest of Europe settled on PAL, developed and deployed its own secure but completely incompatible system called TETRAPOL.[83] Later, France obtained a waiver from the European Union to proceed with TETRAPOL and consequently did not implement the ERC decision.[84] With French support Czechoslovakia, too, opted for TETRAPOL.[85]

---

[80] Ibid. "1. To designate the bands 380–385 MHz and 390–395 MHz as frequency bands within which the requirements of the digital land mobile system be met[.]"

[81] Ibid. "2. [T]hat for the purpose of this Decision a single harmonised digital land mobile standard for emergency services, adopted by ETSI, shall be used in the designated frequency bands[.]"

[82] See http://www.ero.dk/documentation/docs/implement.asp?docid=1493.

[83] TETRAPOL is not a standard recognized by ETSI or the ITU; in fact the ETSI General Assembly rejected the TETRAPOL standard in its meeting of April 22–23, 1999. TETRAPOL's main proponents are French law enforcement agencies as well as French telecom and military hardware vendors.

[84] See the TETRAPOL website at http://www.tetrapol.com.

[85] Czechoslovakia later split into the Czech Republic and Slovakia. The fourth nation not signing on to the ERC decision, Sweden, did not want to dedicate the frequency band (designated by the ERC) exclusively to emergency services.

French exceptionalism, however, cannot obscure what is a success story under any view. Within a single decade, and despite its complex, multilevel decision-making structures, Europe agreed upon and implemented a continent-wide common frequency and a common communications standard based on TETRA technology. Together frequency and standard form the regulatory basis for comprehensive interoperability of public safety organization communications systems in Europe.

(c) Funding: Utilizing Technology to Attract Private Investment

Europe's public safety organizations are in a situation similar to their American counterparts with respect to their communications systems. Most of them still use old analog systems, but they are considering a switch to new digital systems. According to an EU estimate, most European public safety organizations will have moved to an interoperable digital system by 2010.[86] Unfortunately, as in the United States, finding sufficient funding for this replacement is going to be difficult. But unlike the United States and its (temporary) budget surpluses, in Europe nations are still scrambling to balance their budgets in compliance with the Maastricht criteria of monetary union and the ensuing "stability pact." Only very limited public funding will be available and given reduced tax revenues due to the global recession, these dire financial circumstances may continue for some time. The need for substantial capital to rebuild Europe's public safety communications infrastructure thus could hardly have come at a more inopportune time.

Interestingly, however, European governments have not wavered in their commitment to interoperability. Instead, and with the budget crisis as a backdrop they looked at what the new communications networks could offer, not primarily in terms of monetary *needs*, but of monetary *savings*. For example, the Belgian government has instituted the ASTRID program, creating a nationwide TETRA-based digital radio infrastructure to be *shared* by all Belgian public service agencies.[87] This sharing arrangement saves agencies significant amounts of money because it avoids the inefficiency of having multiple networks—one for each agency—covering the same or overlapping geographic areas.

---

[86] See, e.g., ERC, "Harmonisation of Frequencies for Police and Security Services in Europe".

[87] "ASTRID TETRA Network", available online at http://www.mobilecomms-technology.com/projects/astrid/index.html.

Sharing communications infrastructure like transmitters and relay stations is nothing novel. In the United States, some agencies have been sharing infrastructure for years and reports examining potential strategies for funding improvements in communications systems have advocated sharing arrangements as a way of reducing costs.[88] Simple sharing arrangements require that two or more agencies decide to share the cost of building infrastructure. But often procurement cycles and funding opportunities vary among communications agencies. Securing funding—hard already—is almost impossible at any specific moment in time. One could, of course, envision a sharing arrangement in which one agency, having received funding, builds the agreed-upon network and later lets another agency use it, perhaps for a fee. But why should one agency shoulder all the risk in building an infrastructure when it is uncertain that others will join?

This is a fundamental dilemma in funding network infrastructures. The early adopters of a new communications technology bear a higher risk than latecomers. Because it seems acting early does not pay, everybody waits for others to make the first move. Political scientists call this a "collective-action problem."[89]

There are a number of ways that the collective action problem can be overcome. An obvious one is for one agency to shoulder the financial burden when it needs an infrastructure anyway and the cost for permitting others to share is minimal. Or an agency leader may just desire to be entrepreneurial. But these are exceptions. In most cases, public safety agencies have neither the funds nor the entrepreneurial spirit. A more promising solution is to have central coordination: the government steps in and finances the infrastructure buildup, shouldering the risk as a public good. This is precisely what the Belgian government did in the ASTRID program. This solution, too, is not novel. In the United States, numerous state governments have already financed shared communications infrastructure.

[88] See PSWN, *Report on Funding Strategy*, pp. 6-1 et seq.

[89] See Mançur Olson, *The Logic of Collective Action* (1971).

There is an important difference, however, between shared analog (or early digital) communications networks and a shared comprehensive system a la TETRA. Because of the limited number of channels available and the inefficiency of assigning them manually, many of the shared U.S. systems cannot accommodate *local,* only state public safety agencies (the Project Hoosier SAFE-T currently in its early stages will provide a fully integrated trunked digital network for the state of Indiana and is a most laudable exception[90].) Moreover, these systems generally do not manage communications based on message priority, and access to communications channels is purely first come, first served. In an emergency, such networks may quickly produce a lot of noise (communications of limited importance) making it hard for users to filter out truly important information.

By contrast, TETRA and similar systems efficiently manage channels and hence scale well. They are designed to incorporate many different agencies, and with priority codes and the creation of talk groups on the fly guarantee the level of flexibility needed when truly sharing a network among different user groups. Like the packet-switched Internet, TETRA and comparable advanced systems provide a high level of resource efficiency, enabling the infrastructure to be used by many different user groups. In other words, the Belgian public safety agencies using the ASTRID network receive more benefits for less cost than in traditional resource-sharing setups. Building a truly shared digital network involves successfully leveraging a first important technological advantage. But there is more to be gained.

i. Walky-Talky in the Burgenland

The Burgenland, situated right next to the border with Hungary, is one of Austria's poorest states.[91] For thirty years, the state EMS agency had used the same analog radio system to communicate with its seventy EMS vehicles and seven base stations. By 1998, establishing radio communications had become difficult. Hungarian taxicab radio routinely interfered, and a national law constrained the organization from using more transmission power. The equipment was just too old.

---

[90] "Hoosier SAFE-T Communications System—Indiana Statewide Digital Radio System," available online at http://www.mobilecomms-technology.com/projects/indiana/index.html; see also PSWN, *Case Based Tutorials on Shared System Development—Coordination and Partnerships* (December 2001).

[91] The section is based on interviews by the author with Walky-Talky operators, users, and political decision makers

Searching for a new radio system, Walter Adorjan, the EMS agency's radio officer, came across a group of entrepreneurs. Soon they found common ground. In early 1999 Walky-Talky was incorporated. It had a simple mission: to build a statewide TETRA network infrastructure and to let public service agencies use it for a fee.

Having a private company construct and maintain the network infrastructure required for a shared communications system provides a number of advantages over public financing of a shared network. First, it requires no initial investment from the public sector. The network is built by a private-sector actor that arguably has better financing expertise than a public sector organization and a keener desire to keep expenses in check. Agencies are charged a flat monthly fee per radio handset for using the network. This permits them to budget sensibly and to switch to the new network without having to pay up front for all, or even a portion, of the initial investment. Agencies have to purchase handsets[92] (although Walky-Talky has negotiated attractive agreements with Nokia, which operates a research center close by, for leasing handsets). The network provider calculates the fixed monthly fee it charges agencies based on the volume it thinks it can attract, hence not penalizing early adopters. As with all network infrastructures, the setup offers strong incentives to the network provider to sign up agencies to use the service. Although this does not solve the collective-action problem, it shifts it to the network provider, which arguably has better expertise than agencies in how to overcome it. For example, as with other telecommunication markets, fee structures are possible that provide incentives for agencies to switch, and the earlier the switch, the cheaper.

Walky-Talky took in Austria's incumbent telecom provider Telekom Austria and a private-sector arm of the state government as equity partners.[93] In October 1999, Burgenland's EMS agency became Walky-Talky's first customer. In 2000, the network covered in excess of 90 percent of the entire state, with capital investment of little more than $3.5 million. Twenty-five fixed transmitter/relay stations and two portable transmitters were deployed, supporting 600 radios (and growing fast) and their users, from firefighters to law enforcement agencies.

---

in September 2000, with follow-up interviews in November 2001.

[92] Prices for radios range from $400 for a handset radio to $800 for a car radio.

[93] See Peter Martos, "5-Milliarden-Projekt Adonis wird vom Anbieter finanziert," *Die Presse*, October 31, 2001.

Quickly Walky-Talky developed an understanding (and appreciation) for the different usage patterns of public safety agencies and for the way TETRA systems handled traffic. For example, EMS agencies have base-level traffic all day as they tend to routine tasks and smaller accidents. Communication traffic swells in the case of a larger accident. In contrast, the traffic pattern for local firefighter units, consisting mostly of volunteers, is quite different: Ordinarily there is almost no communication traffic, but once there is a fire, dozens and dozens of users have to be contacted at once. Whereas EMS agencies use a communications network continuously, firefighters essentially pay for it being provided in case of an emergency. This leaves a typical public safety network, over-provisioned to accommodate even heavy traffic in case of a large emergency, underutilized. Adding user groups with more continuous communication needs, like EMS or law enforcement agencies, may somewhat balance the load in times of no or only small emergencies. But the benefits of such a balance are lost once a large emergency requires all agencies—firefighters, police, and EMS—to use the radio network very actively.

What Walky-Talky needed, as a supplement to its public safety usage base, were public-sector users that would want continuous, but not time-critical, communication. In times of emergencies, such users would find it acceptable to wait a few seconds (or even longer) for a free channel. Walky-Talky found such users not among public *safety*, but among public *service* agencies with communication needs. Soon, highway gritting trucks were connected, as well as park rangers and environmental protection officers. The TETRA network was used to transmit street temperature and other weather data along the interstate to central command and to control ice-warning signals. With TETRA's built-in capability to prioritize automatically depending on who wants to communicate, emergency agencies do not have to fear that weather data will constrain their communication needs during emergencies.

As we have seen, old analog public safety communication networks are inefficient from an economic perspective: Their capacity is underutilized, except during emergencies. Sharing network infrastructures among public safety agencies, like the Belgian ASTRID network, will at least permit agencies to share the cost of building and maintaining the infrastructure. It will still be underutilized outside of emergencies, but at least every agency will not have to operate its own overprovisioned and underutilized network and instead will share with other agencies. Walky-Talky takes this idea

an important step further. Because of TETRA's communications prioritization capabilities, it can reach out to public *service* agencies, with non-time-critical communication demands, and thus truly balance network traffic loads. The enhanced network efficiency that results from such a balancing translates into higher revenues and, ultimately, lower costs for users. The success of Walky-Talky has prompted the Austrian government to abandon its initial plan, accelerated after the Galtuer tragedy, to construct a shared nationwide emergency communications network. Instead, it has asked the private sector to build it, based on TETRA.[94]

Would it then, one might ask, not make sense to extend the user base of such a TETRA network even further and have private corporations use the network as well? In theory, built-in communication prioritization should ensure that public safety organizations automatically get access to resources (channels) whenever they need to have it, and business users could provide an even better "load balancer" than public service organizations in nonemergency times. Walky-Talky, however, is reluctant to take on private users. It maintains that keeping its market limited to public-sector users is prudent, not the least for marketing reasons. It wants to be successful in convincing agencies to switch to an infrastructure that these agencies do not have immediate physical control over, and it feels that opening up the network to private-sector use might make this task more difficult. Moreover (and more importantly), it points out that across Europe the use of the 400-MHz band is reserved for the public sector.

Walky-Talky in the Burgenland sounds like a fairy tale, and with only 600 radios, the size of the network is limited. A thousand miles northwest, however, the idea of a privately built and run TETRA network for public service agencies is rapidly turning into reality in a nation of over fifty million people. The British government set out to use a funding mechanism similar to that employed by Walky-Talky for the creation and maintenance of a nationwide TETRA-based network infrastructure for Britain. The contract, worth £ 2.5 billion, was awarded to British Telecom (BT).[95] Understanding the economies of sharing a network, and having selected a trustworthy private-sector player to build the infrastructure, the government also decided to boost the new venture with an impressive "launch customer": all police forces in England, Wales, and Scotland. For the next nineteen

[94] Ibid.

[95] "BT Wins Its Biggest Ever Government Contract to Set Up Police Digital Radio Service" (March 8, 2000).

years, BT's TETRA-based Airwave network will provide the communications backbone not just for the police forces. Under the contract's terms, other public safety organizations may contract with BT and use the network. Lancashire's police were the first to use the system in March 2001.[96] By April 2001, Lancashire's fire service had signed on to Airwave and started using it the same year.[97] The rollout to all police forces is scheduled to be completed by 2005, with other public safety organizations added county by county.[98] Liberally defining public *safety* organizations more closely along the lines of public *service* agencies, the British government in 2000 released a long list of agencies permitted to use Airwave.[99] The list was later expanded to include even more public service agencies, like community health professionals and personnel of the environmental agency. In August 2001, the Ministry of Defense signed on to Airwave, extending coverage to additional user groups.[100] The Airwave network will replace aging noninteroperable technology for tens of thousands of users in a nation of over fifty million people, and the public will not have to pay a penny for the initial network buildup.[101]

IV. Enabling Collective Action

The need for public safety agencies to communicate through interoperable radio networks is obvious. Of the three hurdles to developing this capacity identified earlier in this paper, the first—creating the appropriate technology—has turned out to be the least difficult to clear. Agreeing on common rules and creating a suitable funding mechanism, on the other hand, seem to be much more troubling issues (See table 1).

---

[96] "BT's Airwave Service Goes Live in Lancashire Today" (March 19, 2001).

[97] "BT Signs First Airwave Contract With Fire Service" (April 25, 2001).

[98] http://www.airwaveservice.co.uk/Rolloutmap.cfm.

[99] Department of Trade and Industry, "Users of Airwave Allowed Under the License," available online at http://www.airwaveservice.co.uk/attachments/allowedusers.doc.

[100] "MoD Opens the Doors to BT's Airwave" (August 2, 2001).

[101] Similar systems are under construction on the Isle of Man and in Malta. See "Isle of Man TETRA Radio System", available online at http://www.mobilecomms-technology.com/projects and "Malta Mobile Communications Network", available online at http://www.mobilecomms-technology.com/projects/malta/index.html; for a comprehensive assessment of the crucial factors to assess

	Frequency/Standard Hurdle	Funding Hurdle
United States	Deliberative process	Offering some federal funding, and some coordination
European Union	Swiftly setting up frequency and standard	Public-private partnerships

Table 1: Strategies Used to Overcome Hurdles

Underlying these second and third hurdles is the same problem: How does one get a heterogeneous group of stakeholders to act when the ones who take the first step are the ones who may have to pay the highest cost, and thus reap the least benefits? Implementing interoperability requires one to overcome these two distinct collective-action problems.

When Mançur Olson analyzed collective action in his seminal study[102], he discovered that stakeholders would act if they could identify selective benefits and costs. People, he maintains, are joining and working for interest groups and lobbying groups not primarily for the greater good of influencing public policy, but because these groups provide a very concrete, specific service for them. Consequently, public policies requiring collective action have to employ specific strategies to incentivize individual stakeholder action. Very generally speaking, two such strategies have been identified.[103] First, governments can take a "command-and-control" approach, mandating a certain behavior and prompting stakeholders to fall in line either by threatening them with fines or taxes or by inducing them to do so with subsidies. This "type-1" strategy has been the standard public policy fare for many decades. A second type of strategy, that has in recent decades gained some currency focuses less on central decision making and direct financial incentives. Instead, the "type-2" strategy turns to market forces and the private sector to provide an incentive framework. In the area of envi-

fee-for-service networks, and how to best build them, see PSWN, *Fee-for-Service Report* (October 2001).

[102] Olson, *The Logic of Collective Action* (1971).

[103] Recently, a third strategy, called "management-based regulatory strategies," which has not been used either in the United States or in Europe in the TETRA context (and thus will be omitted in this essay) but holds tremendous promise has been added to the toolset; see Cary Coglianese and David Lazer, "Management-Based Regulatory Strategies", KSG Regulatory Policy Program Working Paper no. RPP-2001-09 (July 2001).

ronmental policies, for example, polluters could be prompted to act either by direct regulatory mandates, enforced by fines or the loss of permits. Such strategies represent the "command-and-control" approach. But polluters could also be given "polluting rights" that could be traded on markets. Polluters could invest in cleaner systems and gain financially from selling their polluting rights on the markets to others who continue to pollute but have to pay the price for it. Such an approach is more market-based, and (as it lacks a commanding center) more network-centric. Neither strategy is inherently better in the abstract. The real trick is to select the appropriate strategy for a concrete collective-action problem, taking into account its specific context.

Very different strategies have been used by the United States and Europe to overcome the collective-action problems hampering the move to communication interoperability in the two areas.

(a) Enabling Collective Action for a Common Frequency and Standard

In the quest for a common frequency and standard, at first sight both the United States and Europe chose a traditional command-and-control approach. Yet the authorities in the United States hesitated to exercise their power. Instead, the FCC employed an inclusive, deliberative approach, involving as many stakeholders as possible, and attempted to forge consensus and to accommodate stakeholders even after the fact, as exemplified by its decision to modify its rules once it encountered criticism from stakeholders. Its goal was broad-based buy-in: to convince the stakeholders that interoperability provided each one of them with selective benefits by adding as many of their specific demands (like backward compatibility with legacy equipment) as possible to the overall interoperability policy. In contrast, the Europeans emphasized swiftness of process and the need for a "leap forward," a substantial break with the past. To be sure, stakeholders were involved, but the driving force was a desire to integrate and innovate, even if it meant a break with the past.

Institutionally, the FCC had a strong formal mandate and the unchallenged power to set the rules, yet it opted to facilitate the process more than to drive it. On the other hand, in Europe, players with comparatively weak formal powers—the intergovernmental pillar of the European Union, the ERC, and ETSI—pursued an ambitious course based on central coordination and leadership. This difference is intriguing. Facilitation to prompt buy-in, and strong coordination through central

leadership are common type-1 strategies to overcome collective-action problems. This fact should not surprise us. It is odd, though, that an institution with the power to push for central command-and-control chose facilitation, whereas its European counterparts, relatively weak on formal power, chose the opposite. One would think that neither of them selected a strategy aligned with its abilities. Yet one has succeeded—much more so than the other.

At first, it seems difficult to understand why the Europeans opted for a riskier approach with less power for national stakeholders, especially as the United States, usually more prone to risk taking, pursued the opposite path. Intuitively, one would have guessed things would have worked the other way around. But prior experiences, the path dependencies of the institutional setup, may have played a decisive role. The FCC is attuned to deliberate processes, involving private- and public-sector stakeholders. Taking small, sensible evolutionary steps with long transition stages has played an important role in maintaining predictability and investment security for all involved in areas of FCC authority. It has been the blueprint for formulating regulations governing media and telecommunications, two sectors that have achieved sustained growth. Surely, the FCC must have thought, achieving public safety interoperability presents a similar challenge and will respond to a similar approach.

By the same token, the European institutions, too, remembered their successes.[104] In the late 1980s they picked the fledging Groupe Special Mobile (GSM) standard for mobile telephony, creating a pan-European cellular phone market of tremendous proportions, and establishing a global standard for mobile telephony more successful than any of its rivals. The GSM standard was chosen swiftly, without many years of deliberation. The EU selected it and declared it a winner—and it worked.[105] Enamored with this overwhelming success, the Europeans decided again to pick a winner, and they did. It seems that picking a winner and sticking to it considerably shapes the playing field in favor of the selected. It is not enough to ensure success, but it certainly is of great assistance.

---

[104] The result might have been different if they had also remembered picking losers, like the European digital television standard DMAC; see Xuidian Dai, Alan Cawson, et al., "The Rise and Fall of High Definition Television: The Impact of European Technology," *Journal of Common Market Studies*, vol. 34, no. 2 (June 1996) pp. 149–166.

[105] See Jacques Pelkmans, *The GSM-Standard*, in GOVERNANCE AND INTERNATIONAL STANDARDS SETTING (Walter Mattli, eds., forthcoming).

Understanding this path dependency helps to explain why the United States and the Europeans acted the ways they did when facing essentially the same situation with respect to fostering interoperability of public safety communications systems. It does not explain, however, why one strategy was successful and the other was not. We may have to look at and analyze the third hurdle to do that.

(b) Interoperability Funding: Enabling Collective Action Where It Matters

In the quest to establish appropriate sources of funding, the United States opted for public funding, with federal funds for the early stages. Unlike in selecting a common frequency and standard, the emphasis in funding was more on central leadership and coordination, less on process facilitation. In principle, this seemed an appropriate approach: Federal and state budget surpluses enabled a command-and-control funding approach based on subsidies to be taken. Yet neither Congress nor many of the states decided to offer generous nationwide funding to upgrade public safety agencies' communications networks. Subsidies are a tried and proven strategy to overcome the funding hurdle, but the implementation of the subsidy programs was so haphazard that it largely failed. It was a missed opportunity. U.S. policymakers drastically underutilized the power of their purse (see table 2).

	Frequency/Standard Hurdle	Funding Hurdle
United States	Type-1 strategy, but implementation underutlized available resources	Type-1 strategy, but implementation underutilized available resources
European Union	Type-1 strategy, successful in utilizing available resources	Type-2 strategy, successful in utilizing available resources

Table 2: Types of Strategies Used to Overcome Collective-Action Hurdles

On the other hand, the Europeans opted for a type-2 strategy to overcome the collective action hurdle: an untried market-based approach.[106] Did the Europeans suddenly turn themselves into pub-

[106] It is important to note, however, that such private-pulic-partnerships have very recently become more common

lic-sector entrepreneurs? Unlikely. The European decision was almost completely driven by budgetary constraints. As there were no public funds available to finance the conversion to interoperable systems, alternatives had to be sought. The ingenuity, perhaps uncovered accidentally, was to leverage the power of the technology (a) to share the infrastructure among the stakeholders and more importantly (b) to create a private sector funding opportunity. Innovation occurred when there was no alternative option left. Surely, previous successes in taking risks had whetted their appetite to try a risk-taking approach again.

Clearly, path dependencies are present here as well. They may explain the actions taken, but not why one was a success and the other was not. A key to understanding the European successes lies in the successful alignment of means and ends, of strategies and context.

V. Transatlantic Lessons for Interoperability Policy

A number of important lessons can be learned from this analysis, both for U.S. public policy decision makers, who—especially in the wake of the events of September 11—understand the importance of interoperability and want to correct previous missteps and accelerate the process of achieving it, and for those interested the broader picture of innovation and competitiveness in times of crisis.

(a) Pragmatic Steps toward U.S. Interoperability

Clearly, there is no silver bullet for defining the most appropriate policy to provide interoperability of communications systems for public safety organizations. The best approach depends on the political contexts and on the policymakers' strengths and weaknesses, as well as the type of "selective benefits" that will sway stakeholders to act. It would be shortsighted to transplant to attempt to transplant to the United States the solutions that worked for Europe. The Europeans were successful

in the United States. Four projects, in Florida, Illinois, and South Carolina, as well as through the Federal Specialized Mobile Radio System (FEDSMR) are under way, with the first deployment expected in early 2002; see the insightful report PSWN, *Fee-for-Service Report*.

because the strategy they chose to overcome the two collective-action issues—commonality of frequency and standard, as well as funding—were well aligned with their capacities and the overall political context in which they were operating. They played the cards they were dealt very well.

Consequently, to achieve interoperability (and perhaps sooner than originally planned), U.S. policymakers have to select a strategy based on the available means. For example, given the emphasis on domestic preparedness and homeland security, stakeholders today are clearly prepared to accept more central command and control. As a result, the FCC could now be more forceful than it has been in the past in freeing up frequency spectrum for interoperability before 2007 and in embracing technological standards more attuned to current technological possibilities.[107]

On the funding side, too, changed budget priorities as a result of the war against terrorism may make it feasible to establish more substantial federal and state-sponsored interoperability funds than before. Offering subsidies to tens of thousands of public safety agencies that make interoperability-related investments provides a very immediate "selective benefit" and will prompt them to act. Given the selected standard and the power lineup, this seems to be the most sensible strategy. Alternatively, one could of course also envision a market-driven funding strategy, akin to Britain's Airwave initiative or Walky-Talky. For such a type-2 strategy to succeed, however, the interoperability standard would probably have to be amended to ensure calls could be prioritized (the prerequisite for sharing the infrastructure among public *service* agencies).

(b) Broader Lessons for Innovation through Public Policy

But there is more to the story. Perhaps one ought to look not so much at what differentiates the European strategy for establishing a common frequency and standard and for obtaining the necessary funding from the ones in the United States than at what the two European strategies have in common. The Europeans overcame the standards hurdle and the funding hurdle by opting for less conventional, riskier solutions. Instead of deliberations, they swiftly identified and declared a "win-

[107] The post-September 11 declaration of Project 25 and TETRA representatives that they will work toward a joint standard may be an early indication for some forward movement in these areas.

ner." This tactic can be dangerous, because they could have picked the "wrong" standard, a technologically inferior one, or one too advanced, requiring too much adaptation at too high a cost. But it seems that the sheer fact of picking a winner, announcing a strategy and sticking to it created an environment conducive to success. Similarly, the funding hurdle seemed insurmountable. The Europeans succeeded in overcoming it by not attacking it through traditional means, and instead opting for an alternative, untried strategy. They took, perhaps out of necessity, the riskier route. In sum, the European strategies to overcome each of the two collective-action problems were similar. They were well aligned with, and reinforced, each other. The success the strategy chosen for taking one hurdle bolstered the belief that that was the way to take the second as well.

Moreover, the Europeans aligned their overall strategy well with the first hurdle: technology. Unlike in the United States where technology seemed to be either a given or something to be decided by consensus, the Europeans chose a technology that permitted them to overcome another obstacle, the funding hurdle. Traditionally one would see little connection between the choice of technology and the funding structures (apart from the amount of money needed to acquire the technology chosen). Only by leveraging the unique properties of digital trunked networks could the Europeans create an opportunity for the successful public-private partnerships we have seen. The European perception that technology is not an external constraint or an unrelated decision, but intricately linked to the social context of its use, reinforced the belief that interoperability requires a clear, comprehensive strategy. The United States, on the other hand, used two very different strategies to take the two hurdles. Hence, no similar strategic reinforcement could occur. Thus, a much broader (and perhaps simpler) lesson can then be drawn from the case of developing interoperability in public safety communications: When faced with interconnected collective-action problems, it may be most advantageous to devise a comprehensive strategy to tackle the entire issue, and not just distinct parts.

VI. Conclusions

This paper has analyzed the activities in the United States and Europe over the last decade designed to solve the complex problem of interoperability of public safety organization communications systems. It has identified three hurdles that have to be overcome to make such interoperability a reality: technology, common frequency and standard, and funding. I have laid out the major debates for each of these hurdles on both sides of the Atlantic and their internal dynamic. So far, the Europeans are clearly ahead of the United States in the quest to implement such interoperability.

Policymakers concerned about interoperability may want to take a page from the European strategy and understand the importance of strategic alignment. The FCC could modify its stance and actively pursue an accelerated move toward a common frequency and standard. Federal, state, and even local government could reassess its priorities and decide to fund a substantial part of the cost of transition from current systems to interoperable ones, under the assumption that interoperable communication networks are a "public good." Putting bruised egos aside, these may be the best options to put interoperability back on (the fast) track.

Policymakers more generally concerned with overcoming collective-action problems, as one frequently encounters in the network economies, may benefit from understanding the spectrum of solutions tried on the path to interoperability and their successes and failures. Examining the European strategy, the ingredients for its success become obvious: Strong agency leadership, intentional risk taking, and public entrepreneurship were combined in a comprehensive overall strategy. It created a reinforcing belief in winning and the understanding that one may pick technology based on future requirements, not present needs. Leadership and risk-taking entrepreneurship are not generally associated with Europe. But previous successes in both have made the Europeans more American. Strangely, the Americans—risk-averse, deliberative and haphazard—seem to have become more European. These are core lessons to be drawn from a decade of interoperability policy. Instilling leadership, the willingness to take risks, and the ability to create comprehensive strategies into the U.S. policy machinery may be the most promising long-term approach to public management, and the most needed one.

But one must never forget: Leadership, risk-taking, comprehensive strategic thinking are the tools. The goal of interoperability is to have firefighters communicating seamlessly with their brethren from EMS, with policemen and women, and with the innumerable other first responders. When on September 11, 2001, the Pentagon stood ablaze, almost a decade after the first World Trade Center bombings, and years after Columbine High, responding fire companies from Maryland once again could not communicate with those from Washington, D.C. and Northern Virginia.[108] Runners had to be used instead—a shocking reminder of a crisis unsolved.[109]

[108] See Steve Twoney and Carol D. Leonnig, "Rush Is On to Boost Region's Response to Terror Attacks," *Washington Post*, September 30, 2001, p. A01.

[109] The tragedy of 9/11 holds many lessons for interoperability. Yet, at the time of this writing (2002) only portions of the primary materials are available. Once complete transcripts of the emergency communications at WTC have been made public, and detailed reports have mapped out and assessed the brave efforts of the first responders, many of whom gave their lives, they will surely teach us many more powerful lessons on how to improve communications interoperability.