# Comments of Swissphone Telecom on the FCC's Ninth Notice of Proposed Rulemaking, FCC 06-181, Released: Dec. 20, 2006

Swissphone is a private company that was founded in 1969 by Helmut Köchler to minimise miscommunication and accelerate quick, joint responses to emergencies.

The FCC's 9th NPRM is welcomed because it prompts local, state and federal government entities – and everyone else in public safety – to find a way out of their worsening communication crisis.

Contrary to what the FCC's 9th NPRM assumes:

- the safety of the public does not depend on established organisations only (see Section 1: *Who's in charge? In a disaster, nobody)*,
- compared with day-to-day emergencies, mutual aid has a growing importance,
- there is no technical or administrative way to prevent wireless broadband and interoperable equipment from permeating and being permeated by cyberspace.
- established organisations in public safety do not need a new, large-scale network purpose-built for broadband. What they need instead is the nerve to use the broadband that accommodates everyone.

The recommendations herein take recent disaster research into account and are for a realistic public safety performed by officially recognised organisations, commercially motivated and non-profit emergency managers and the public themselves.

Swissphone Telecommunication AG
Edouard Dervichian
21 Fälmisstrasse
CH-8833 Samstagern
Switzerland

edouard.dervichian@swissphone.com

# Contents


1 Who's in charge? In a disaster, nobody. ....4
1.1 Day-to-day emergencies ....7
1.2 Mutual aid ....8
1.2.1 DRC typology of organisations in mutual aid ....9
1.3 Recommendation: Ask incisive questions ....11

2 Broadband accommodates everyone ....13
2.1 Recommendation: Consider all methods of communicating ....13

3 Emergency management: sharing vital information and communicating warnings ....15
3.1 Government and private emergency managers ....16
3.2 Sharing information ....16
3.3 Voice ....17
3.4 Warnings ....18
3.4.1 The basics of warnings ....18
3.4.2 Warning emergency personnel ....18
3.5 Broadband connectivity ....21
3.6 Recommendation: Exempt essential broadband from licensing ....22

4 Methods of communicating for the safety of the public ....23
4.1 The three technical approaches to sending information ....24
4.1.1 Case 1 - The broadcasting approach ....24
4.1.2 Case 2 - The purpose-built, common node approach ....25
4.1.3 Case 3 - The demand-guided approach ....25
4.2 Towards independence from nodes ....26
4.3 This is cyberspace! ....27
4.4 What is a cyberspace disruption? ....27
4.5 Is there any certain precaution against the hazards of cyberspace? ....28
4.6 Recommendation: Recognise the hazards of cyberspace ....29

5 The safety rules of warning ....30
5.1 Weight of sent information ....30
5.2 Vital warnings ....31
5.2.1 Meaning and the lack of meaning ....31

5.2.2 Reducing the risk of miscommunicating warnings ....31
5.2.3 Loss of network and the illusion that ends are safe ....32
5.3 Radiopaging ....34
5.4 Recommendation: Follow a sound warning doctrine ....35

6 Comments for spectrum utilisation - *ad hoc* broadband ....36

I INTRODUCTION ....36
II BACKGROUND ....40
III DISCUSSION ....41
A. Objectives of Public Safety Model ....41
B. Proposal ....46
1. Single National Public Safety License ....47
Interoperability in misleading terminology and in sane English ....49
4. Requirements of the National Public Safety Network ....50
6. Unconditional Preemptible Access to Commercial Service Providers and Joint Provision with Commercial Services ....54

Bibliography ....56

1 On disaster research ....56
2 On communication ....57
3 On the original motif for US radio communication law ....57
4 Federal Communications Commission proceedings ....57
5 On communication failures that were fatal ....57
6 On snazzy approaches to broadband ....58
7 On unabated technological hubris ....59
8 On combating technological hubris ....59

About Swissphone ....60

# 1 Who's in charge? In a disaster, nobody.

*There is a need not only to note but to accept the fact that since all disasters are initially and essentially social occasions, planning for them has to be primarily by social means.*

[E. L. Quarantelli – *Programs and policies that ought to be implemented for coping with future disasters,* University of Delaware, Disaster Research Centre, 2003]

Public safety work is either ***day-to-day*** or ***mutual aid***. In the former, someone is usually in charge; in the latter, however, it is simply not possible for any one person or organisation to be in charge of the whole works.

The FCC's 9th NPRM is written about grappling with ***day-to-day*** emergencies only – it does not consider ***mutual aid*** at all, e.g. mass casualty disasters, catastrophes or big projects like major rallies and sports events.

It is erroneous to assume that public safety is done by officially recognised organisations only. Indeed, members of official organisations are not even usually the first to respond. Government entities on the scene need the help of other people – and the greater the problem the more such help is needed. Dozens of private organisations can be involved.

Unless officially recognised organisations use the ubiquitous broadband they will exclude themselves from communicating criss-cross with all other organisations or persons spontaneously[1] or professionally involved in public safety.

[1] See, e.g., Averill, D. et al., 2005. *Federal Building and Fire Safety Investigation of the World Trade Center Disaster – Occupant Behavior, Egress, and Emergency Communications*, Building and Fire Research Laboratory, National Institute of Standards and Technology, September 2005, at page 151, available at: http://wtc.nist.gov/NISTNCSTAR1-7.pdf

For everything other than alerts and voice, the FCC must urge officially recognised organisations to use the broadband that is already available and that increasingly accommodates more and more of the world's population.

Tragically, day-to-day emergencies like road accidents claimed more than 42,000 lives in the USA in 2003 - far more than most mutual aid occasions. Nevertheless, the FCC must accommodate everyone who might ever need to communicate for mutual aid, because the potential for really huge disasters is greater than ever before.

A crisis is a breakdown in the ability to construct meaning.

In a disaster, technology has no use until the people involved become able to construct at least some meaning.

For hazards with rapid onset, close proximity or both the most effective means of warning is a combination of one-way (i.e. radiopaging, sirens) and two-way communicating technology (i.e. telephony, GSM, Project 25, WiMax). Two-way alone is inadequate unless the available warning time is at least an hour (Mileti et al. 1990).

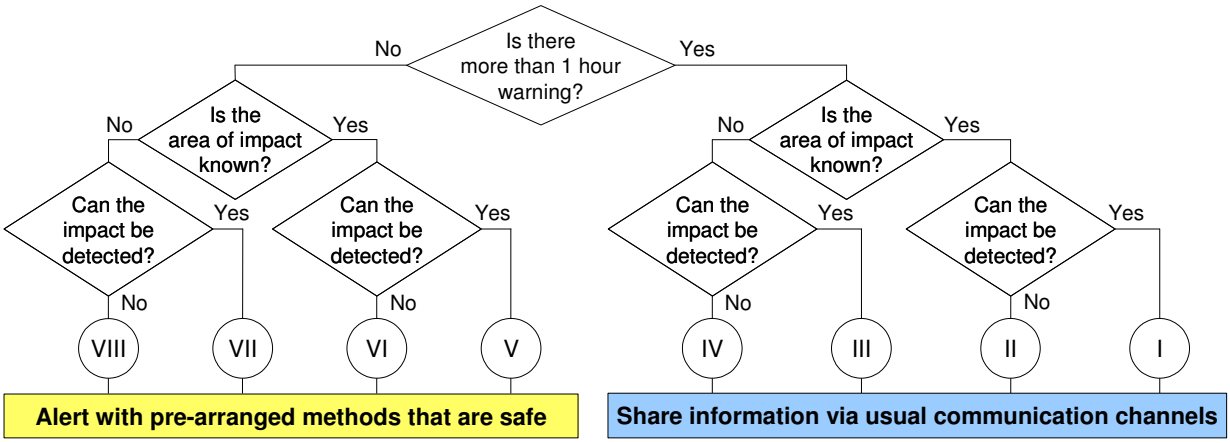
Table 1.1 shows which technology is likely to remain effective in a disaster. Nation-wide radiopaging networks, and mobile communication networks, fail when the underlying telecommunication network fails. The essential, quick alternatives are end-to-end communication methods (e.g. local end-to-end radiopaging, on-site paging, sirens, walkie-talkies, satellite, flags).

Before any disaster hits, it must be settled which of the existing communication methods are appropriate to:

1. determine whether an emergency has occurred,
2. maintain prescribed response times,
3. not alarm the public unnecessarily, and
4. link to other organisations, sectors and areas.

Table 1.1: Comparison of the effectiveness of technologies for sending vital information

**Mileti et al's (1990) grouping of hazards**

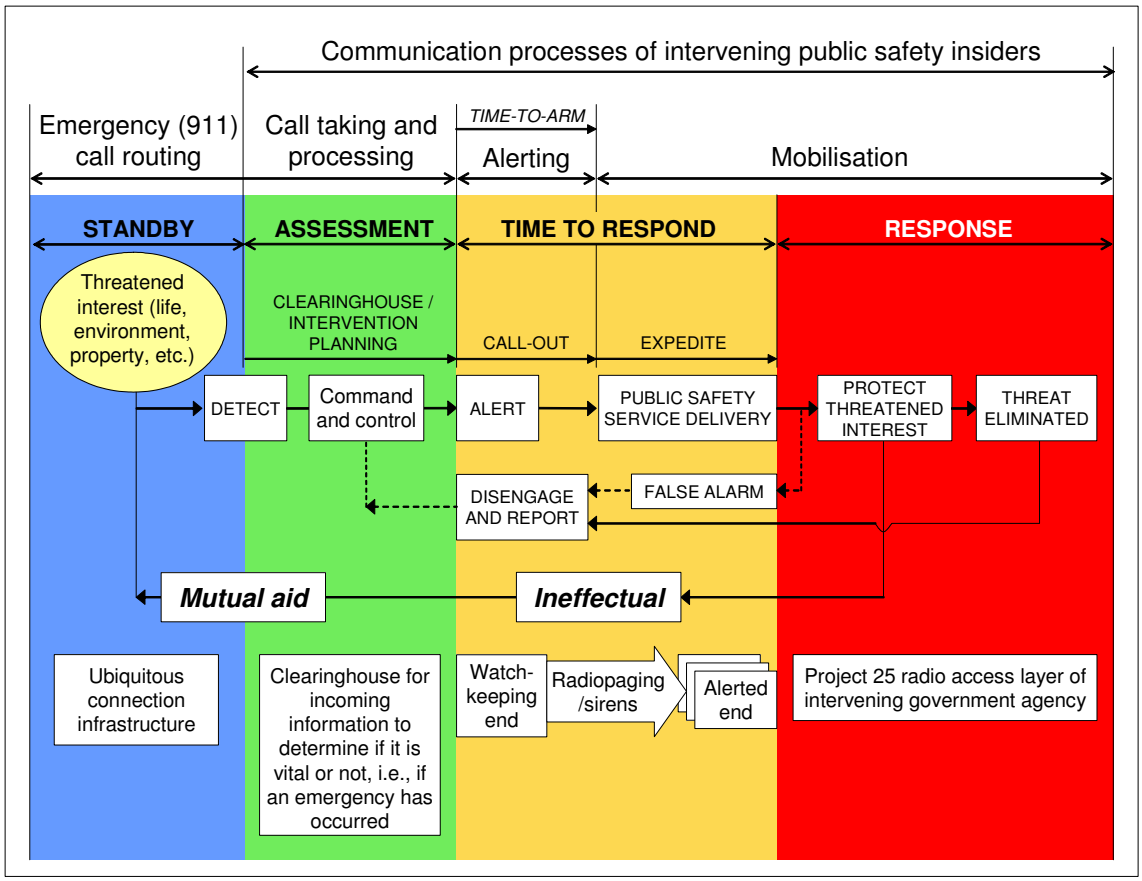



| | Radiopaging and walkie-talkies | | | | Interoperable equipment | | | | For warning and informing the public | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Useful for warnings of hazard types; | VII & VIII | VI | V & VI | Allround | I & IV | II & III | III | III & II | I & IV | I & IV | V & VI |
| | Nation-wide radiopaging | Local, end-to-end, radiopaging | On-site paging | e2e walkie-talkies | US Project 25 radios and EU TETRA radios | Mobiles (GSM, G3, WiMax, Wi-Fi, etc) | *Ad hoc* wireless broadband | Telephone ( POT & VoIP) and messaging | Terrestrial broadcast TV | Broadcast radio | Siren for advanced warning |
| Earthquake | | | | | | | | | | | |
| Flood | | | | | | | | | | | |
| Cyberspace failure | | | | | | | | | | | |
| Power failure | | | | | | | | | | | |
| Terrorist attack | | | | | | HTR | | HTR | | | |
| Wind storm | | | | | | | | HTR | | | |
| Big fire | | | | | | HTR | | HTR | | | |
| Major transport accident | | | | | HTR | HTR | | HTR | | | |
| Chemical accident | | | | | HTR | HTR | | HTR | | | |
| Nuclear accident | | | | | HTR | HTR | | HTR | | | |
| Cosmic troublemaker | | | | | | HTR | | HTR | | | |
| Key | Destination can be reached | | | | HTR = Destination is hard to reach | | | | Destination is out of reach | | |

## 1.1 Day-to-day emergencies

Day-to-day emergencies are those managed with routine procedures and resources.

In general, the delivery of day-to-day safety services by local government entities is managed using some or all of the heterogeneous communication procedures shown below.




This model of managing emergencies is barely adequate for day-to-day. It certainly does not work on mutual aid occasions, when officially recognised organisations trying to protect threatened interests need to communicate with organisations that do not have – *and do not want to have* – Project 25 radios.

## 1.2 Mutual aid

A mutual aid occasion is one not manageable using the routine procedures and resources of government[2].

From the perspective of government, three levels of emergency give rise to mutual aid:

- *Local emergency*

  disaster conditions or extreme peril to the safety of persons and property within the territorial limits of a municipality or city, which are, or are likely to be, beyond the control of the services, personnel, equipment, and facilities of that municipality or city, and which require assistance from elsewhere.

- *State of emergency*

  disaster conditions or extreme peril to the safety of persons and property within a province which, by reason of their magnitude, are or are likely to be beyond the control of the services, personnel, equipment, and facilities of any single city or province, and which require the combined forces of neighbouring regions.

- *State of war emergency*

  the condition that exists immediately when the nation is attacked by an enemy or is warned by its government that such an enemy attack is probable or imminent.

[2] See, e.g., Oral Testimony of Commissioner Steven M. Gregory, Federal Communications Commission, PSNCC General Membership Meeting, Transcript at pp. 41-53 (November 16, 2001), available at November 16, 2001 General Membership Meeting Transcript

### 1.2.1 DRC typology of organisations in mutual aid

The Disaster Research Center (DRC) in Delaware classifies organisations that offer mutual aid in an emergency according to their tasks (regular/non-regular) and structure (old/new).

| | | TASK | |
|---|---|---|---|
| | | Regular | Non-regular |
| STRUCTURE | Old | Type I<br>Established organisation | Type III<br>Extending organisation |
| | New | Type II<br>Expanding organisation | Type IV<br>Emergent organisation |

**DRC typology of organisation that appear during a mutual aid occasion**

When these four types of organisations work alongside one another, meaning cannot simply be 'transmitted' but has to be constructed *ad hoc* by initiators and interpreters.

E.L. Quarantelli (1999), Professor Emeritus of the University of Delaware Disaster Research Center (DRC), states that in a disaster:

> *… there will be Type IV groups who will be undertaking necessary tasks, and that there will be Type II and Type III organizations operating as well as established ones using their regular social structure to carry out old tasks (e.g., police departments directing traffic and maintaining security in the community). A response that tries to involve only established organizations* [Type I] *is a clear indication that there has been poor disaster management.*
>
> *In both the proscriptive and research literature on disaster management, it is often said that there are "communication" problems at the crisis time of disasters. Such a formulation, however puts an emphasis on communication technology, the means used rather than what is communicated. Thus, for*

*example, there are statements made that "more radios" are or were needed. However, research shows that most problems stem from what is communicated rather than how communication occurs. In most cases, information flow problems do not arise from equipment scarcity, damaged facilities, or other forms of destruction that result in rendering the communication technology inoperable. They stem more from problems in the process of communication itself, the information flow per se.*

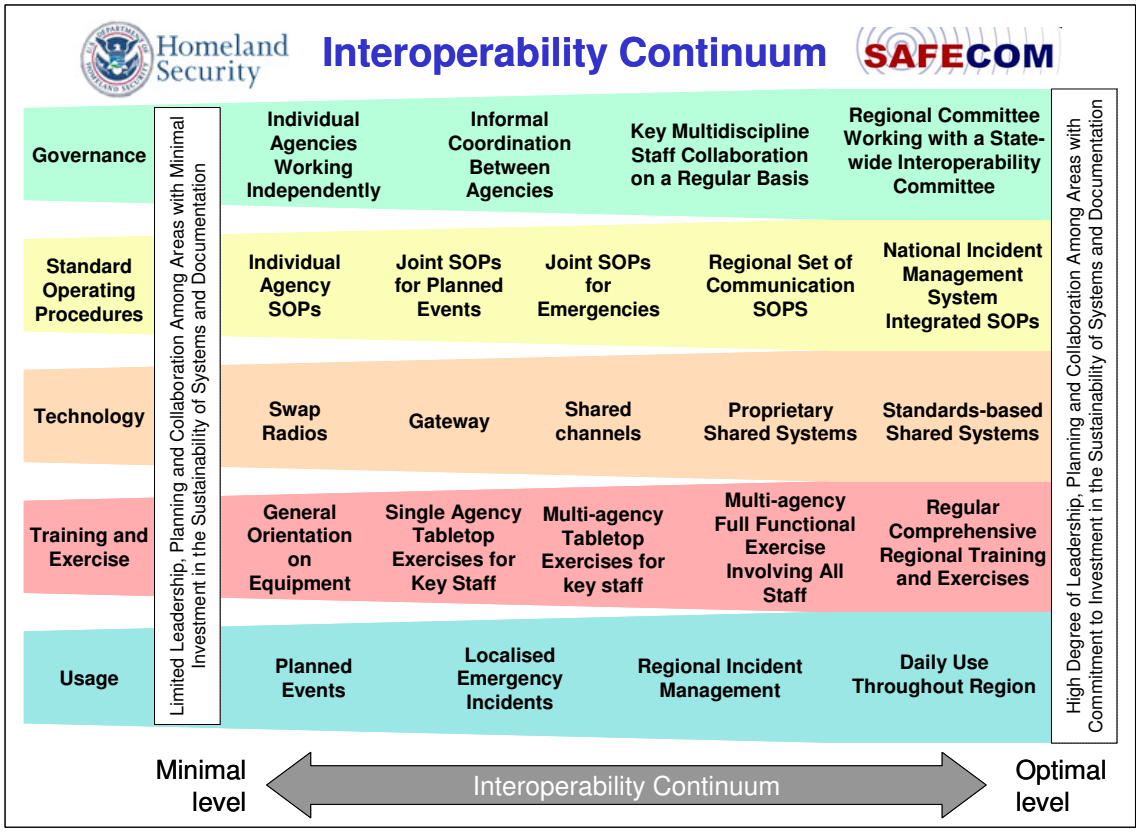
*Necessarily there are multi streams of information flow during the crisis period of a disaster. There is the information flow:*

*within every responding organization;*
*between organizations;*
*from citizens to organizations; and*
*from organizations to citizens.*

*These information flows can all become problematical in disastrous occasions.*

## 1.3 Recommendation: Ask incisive questions

The importance of mutual aid is growing and many recent mutual aid occasions have proved that it is inappropriate for officially recognised organisations to be dependent on cloistered networks[3] like Project 25. The FCC must therefore courageously pose incisive questions about the DHS's exorbitantly expensive Interoperability Continuum.




1. Does it allow for DRC Types II, III and IV organisations to work alongside established organisations (DRC Type I) with no one in charge?

2. Are "Standard Operating Procedures" *standard* because they are known by whoever you might run into?

3. Are "Standard-based Shared Systems" *standard* because they are known by everybody?

[3] See, e.g., *Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks* – Report and Recommendations to the Federal Communications Commission June 12, 2006 pp. 7-8, available at http://www.fcc.gov/eb/hkip/karrp.pdf

4. Are "Standard-based Shared Systems" *shared* because they are used to interact with everybody?

5. Can "Standards-based Shared Systems" avoid relying on one or two vulnerable common nodes besieged by cyberspace?

6. Will the Continuum lower social inhibitions to sharing information in times of 'normalcy'?

7. Does the Continuum acknowledge that it is logically and technically impossible to control the information-sharing between everyone who is involved in a disaster?

8. Will it improve the quality of information shared during a disaster?

9. Does it preserve analogue, push-to-talk, e2e, radiocommunication?

10. Does it aim to accommodate everybody's broadband?

11. Does the Continuum foster realistic expectations about how long it takes to construct meaning fully[4], especially in a crisis?

A 'no' to any of these questions means that the Interoperability Continuum is unsuitable for mutual aid.

The Interoperability Continuum is an attempt to plan for the communication that takes place in a crisis (i.e., when the ability to construct meaning has broken down). This kind of planning is, at best, applicable to day-to-day emergencies. *Force majeure*, however, can force one to have to gather facts before any response is possible. In fact, there is only an indefinable line between day-to-day and *force majeure*.

The FCC must allocate spectrum for mutual aid, because communication is done to organise and not the other way round.

[4] See, e.g. Weick, Karl, 1993. *The Collapse of Sensemaking in Organisations: The Mann Gulch Disaster*, Administrative Science Quarterly; 38 (1993) pp 628-652, a*vailable at*: http://projects.ischool.washington.edu/ ... weick-mann.gulch.pdf

# 2 Broadband accommodates everyone

The safety of the public is everybody's business. It is not the exclusive domain of officially recognised organisations, nor even of homeland security.

Rules governing bringing wireless broadband into disaster impact areas or the daily working environment of public safety must not impede the ability of anybody to connect before, during and after a disaster.

The FCC's 9th NPRM assumes that someone somewhere (the licensee) will be able to control who is on the network. This – were it possible – would prevent the ends from getting on with it by themselves. Broadband devices can build a network quickly wherever placing wires, masts and antennas is ecologically or economically undesirable, too time consuming or simply impossible.

Broadband, whether wireless or not, is used *ad hoc* wherever it is found.

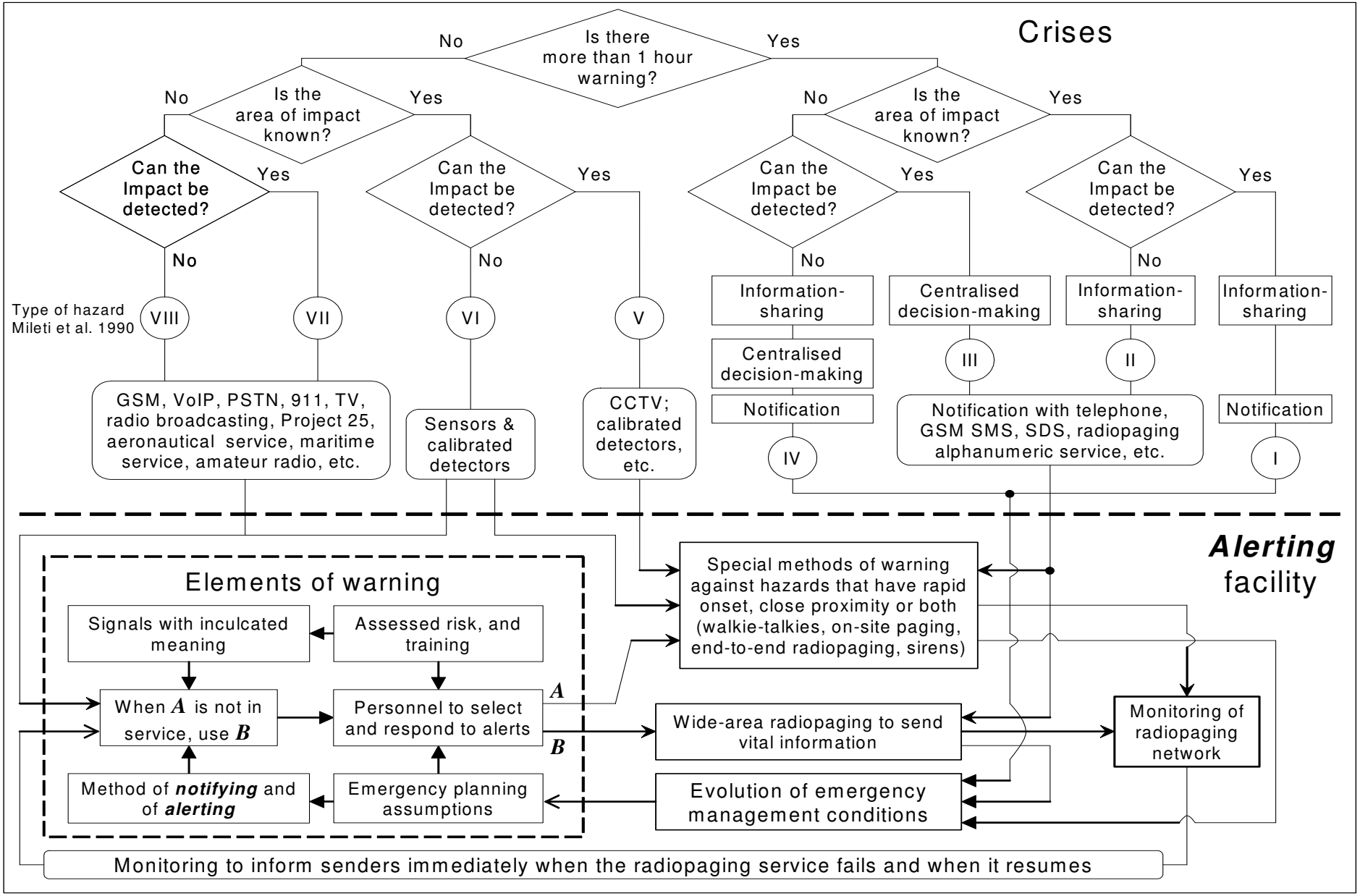
Already broadband is used such that wireless connectivity:

1. is established by ends using only information that is available locally, without the help of any common node,
2. makes short and long range hops,
3. decreases the information throughput whenever it is necessary to increase range, and
4. is used for transit or terminating/originating traffic and not just for uplink/downlink.

These features mean that the terminals actually make the network by themselves, quickly, and as they go along. They allow for the happenstance of sharing vital information on mutual aid occasions.

## 2.1 Recommendation: Consider all methods of communicating

Henceforth, rules affecting public safety communication – also broadband – must not be made in isolation, so as not to jeopardise safety. The FCC is urged to take into account the way hazards are grouped and warnings are issued (see page 14).




**How hazards are grouped and warnings are issued**

# 3 Emergency management: sharing vital information and communicating warnings

The FCC's 9th NPRM is founded on the flawed premise that public safety is done by officially recognised organisations only and that these need large-scale purpose-built networks. This model rejects participation by organisations that are not officially recognised[5] – and play a very significant role in keeping the public safe.

Emergency management means sharing vital information and communicating warnings when something goes wrong.

Public safety involves a lopsided sharing of responsibility between the citizens, and diverse emergency managers and law enforcement officers. Emergency management and law enforcement are radically different even though both rely on the communication of various kinds of warnings.

[5] See, e.g., Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks – Report and Recommendations to the Federal Communications Commission, June 12, 2006 pp. 15-17 and pp. 34-37, available at http://www.fcc.gov/eb/hkip/karrp.pdf.

## 3.1 Government and private emergency managers

Across the world there is increasing privatisation of all sorts of functions previously assigned to governments. Safety, health and the environment are also no longer the exclusive responsibility of officially recognised organisations, and the private and not-for-profit sectors are increasingly involved in emergency management – a new profession growing out of academic teaching, savvy research and practice.

These new emergency managers know that there are now more and worse disasters, and they want clear facts so they can decide:

1. which disasters to deal with,
2. with whom to associate,
3. what to observe and monitor,
4. how they will notify and alert one another quickly whenever there is a threat, and
5. with whom to stage a joint response to observed dangers.

As long ago as 2000, Quarantelli pointed out that:

> *…we are seeing the future of emergency management right now. It is a future characterized by rapidly changing information technologies, a growing body of scientific and technical information on current and future hazards, increasing demand for trained and experienced emergency managers, and the development of a global community of emergency management professionals. It is also a future characterized by new and better tools for decision making, increased pressure on emergency management agencies to be innovative and responsive…*

The FCC must consider everyone who is involved and the most basic means of communication used to share information in life-and-death situations (i.e. ***voice*** and ***warnings***).

## 3.2 Sharing information

Facing common problems and threats does not always justify unlimited information-sharing between emergency managers and law enforcement officers or between the private and public sector.

Sharing information is always

1. first a matter of constructing meaning, and then secondly a matter of connection (i.e. think before you speak),
2. an intimate social contract, once it is embarked upon, and
3. deliberately restricted by social conventions to a group, discipline, community, area or a specific sector.

## 3.3 Voice

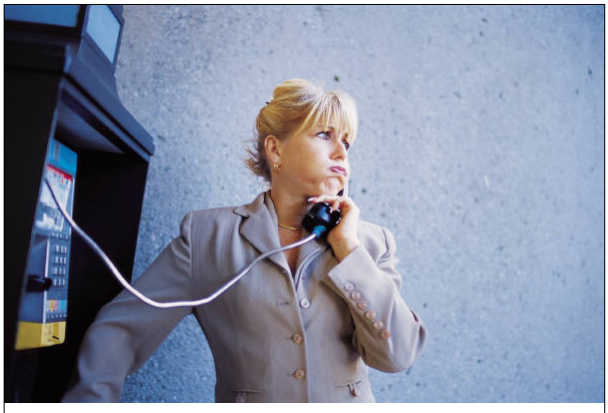
*For communications professionals audio is a different but very powerful tool that we use for observation and situation assessment.*

*Audio transmissions provide us with a broader perspective of an operation, and it forces us to use our minds to draw a picture of what we hear.*

[Oral Testimony of Fireman Steven M. Gregory, Federal Communications Commission, PSNCC General Membership Meeting pp. 41 (November 16, 2001)]

Voice encapsulates significant sound, extension of meaning, simplification of form and division of labor between speaker and listener.

Significant sound



simplification of form with extension of meaning

division of labor

Push-to-talk analogue radios (end-to-end walkie-talkies) are essential for conveying reality on-site where there's trouble.

## 3.4 Warnings

### 3.4.1 The basics of warnings

The basics of warnings are enshrined in doctrine. Doctrine is old stuff that is always extremely helpful.

> *Now, brothers and sisters, if I come to you speaking in tongues, how will I help you unless I speak to you with a revelation or with knowledge or prophecy or teaching? It is similar for lifeless things that make a sound, like a flute or harp. Unless they make a distinction in the notes, how can what is played on the flute or harp be understood? If, for example, the trumpet makes an unclear sound, who will get ready for battle? It is the same for you. If you do not speak clearly with your tongue, how will anyone know what is being said? For you will be speaking into the air. There are probably many kinds of languages in the world, and none is without meaning. If then I do not know the meaning of a language, I will be a foreigner to the speaker and the speaker a foreigner to me.*
>
> [First Epistle of Paul the Apostle to the Corinthians, Ch.14:6-11]

The meaning of warnings must be *inculcated* for *insiders* (associates, those that are in trouble, the invited, allies, etc.). There must also be a way of warning *outsiders* (foreigners, those that are not in trouble, the uninvited, enemies, etc.) meaningfully.

### 3.4.2 Warning emergency personnel

Law enforcement and emergency management personnel can be warned of impending danger by two distinct modes of communication:

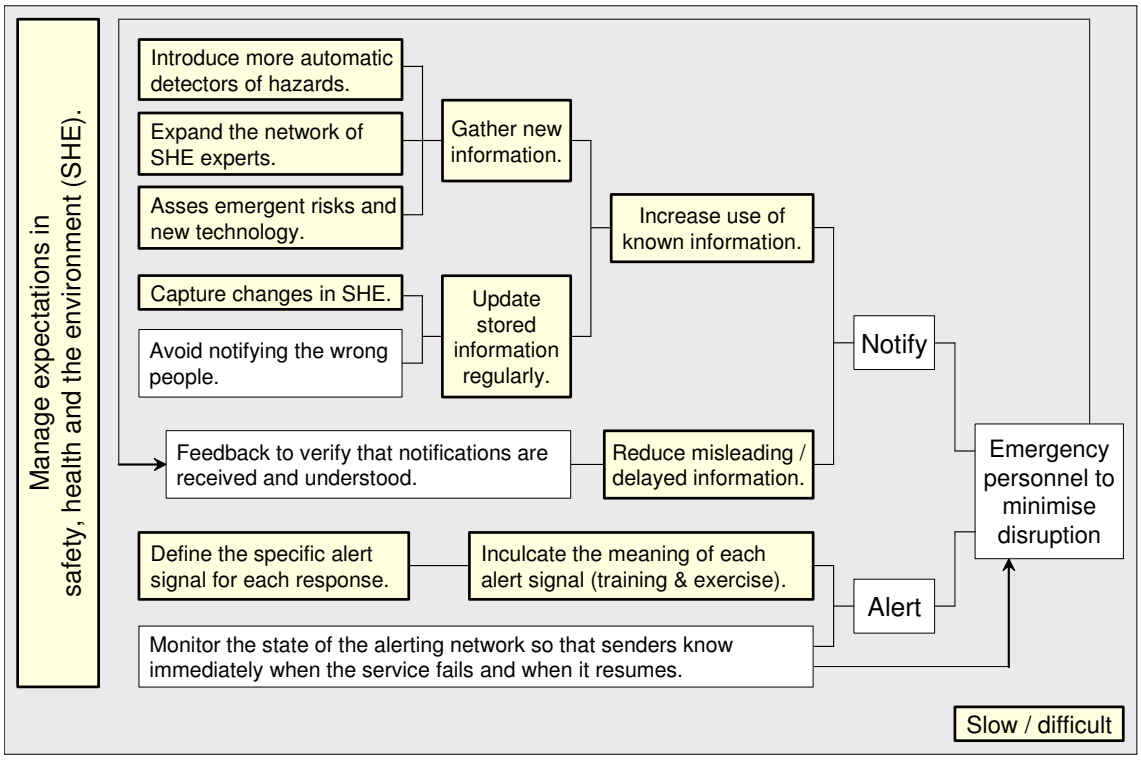
- *Notifying*

  involves creating and conveying a message for which there is no inculcated meaning. The recipient will respond to the warning only in as far as the notification is understood.

- *Alerting*

  is the ability to capture attention. It prompts recipients to engage immediately in the activity inculcated long before the signalled alert is used. This reduces the risk of miscommunication.

Notifying and alerting entail different ways of constructing meaning. In notifying, meaning is constructed as you go along, whereas an alert activates a meaning constructed beforehand.



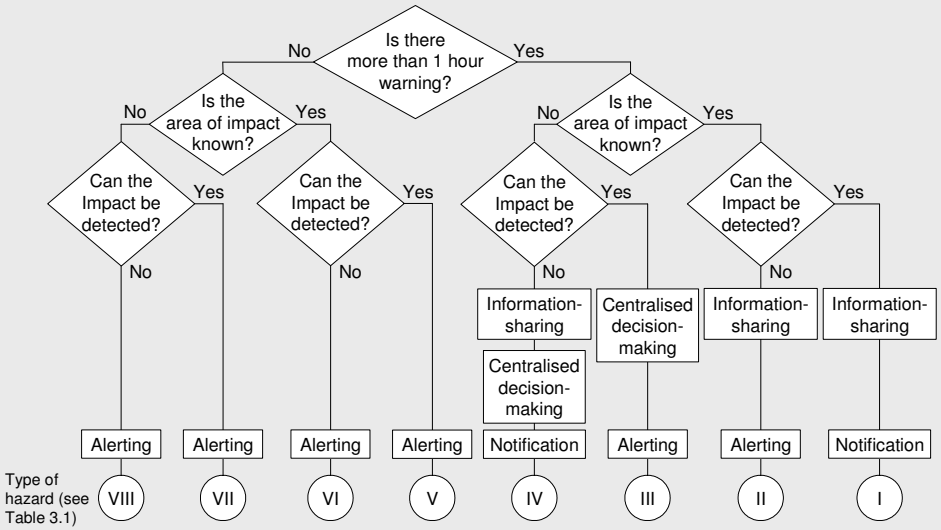

**How warnings are produced, verified and issued**

Alerting associates different organisations through the processes of hazard detection, identification, authentication and connection.

Organisations associated by alerting form a community. The design of an alerting facility must prevent eavesdropping and not alarm community outsiders or the public unnecessarily.

Meaning is constructed, and warnings are communicated depending on the type of hazard. Mileti et al.'s (1990) grouping of hazards provides a basis for deciding how and when to warn (see next page).

| Table 3.1: Where warnings are relevant | | | |
|---|---|---|---|
| Type of hazard | | Hazard | Construction of meaning & how and when to warn |
| I | Long predication time; known impact; easy to detect | | |
| | Meteorological | Slowly developing flood | Emergency responders have enough time to put a plan into action and to warn the public. Notifying is necessary; alerting is unnecessary. |
| | Geological | Ideal earthquake prediction | |
| | Technological | Slow dam failure; gradual nuclear power plant accident | |
| II | Long prediction time; known impact; hard to detect | | |
| | Geological | Earthquake prediction | The onset of the disaster is sudden even though there is a long lead time. Notifying is necessary; alerting is necessary. |
| | Technological | Three Mile Island-type accident; slow fixed-site hazardous materials; erroneously / maliciously corrupted information processed by computers | |
| III | Long prediction time; unknown impact; easy to detect | | |
| | Meteorological | Tornado | Decision-making and management of information is centralised. Notifying is necessary; alerting is necessary. |
| | Geological | Distant tsunami | |
| IV | Long prediction time; unknown impact; hard to detect | | |
| | Meteorological | Drought, global warming | It is important to reach consensus so that the public is informed correctly. Notifying is necessary; alerting is unnecessary. |
| | Technological | Hazardous material threat (DDT & other banned insecticides, asbestos, etc.) | |
| | National security | Nuclear attack; protracted terrorism | |
| | | | |
| V | Short prediction time; known impact; easy to detect | | |
| | Meteorological | Avalanche in ski areas; locations subject to flash flooding, etc. | Calibrated detectors are used to trigger specialised devices (sirens, pagers, etc.). Alerting is necessary. |
| VI | Short predication time; known impact; hard to detect | | |
| | Meteorological | Flash flood | Sensors and calibrated detectors are used. All means of communication, including sirens, are used. Alerting is necessary. |
| | Geological | Fast volcano | |
| | Technological | Fast release of fixed-site hazardous material | |
| VII | Short predication time; unknown impact; easy to detect | | |
| | Sociological | Civil unrest; cyberspace disruption | Emergency call service (US 911, EU 112) and alerting are necessary. |
| VIII | Short predication time; unknown impact; hard to detect | | |
| | Meteorological | Tornado; avalanche | Construction of meaning breaks down. Unlike hazards of Type VI, Type VIII hazards exist across geography. Alerting is necessary throughout the country and internationally. |
| | Geological | landslide; local tsunami | |
| | Technological | Hazardous material release; controlling computer malfunction in, for example, a major power plant. | |
| | National security | Nuclear attack; terrorist attack; sabotage, cyberspace attack | |




Alerting happens when the sender and the receivers carry out an activity which has been rehearsed before the alert is ever used. The meaning of each signal that can be selected for alerting is inculcated so that, depending on the type of hazard detected, the sender sends the right signal to the right group, so that the receivers respond in the right way.

For certain impacts detection is automated and the sender is a computer.

Grouping of hazards - based on Mileti et al. (1990) – a basis for deciding how warnings must be issued

## 3.5 Broadband connectivity

The original rationale for developing broadband lay in its optimal use of marginal conveyance capacity. Now, real-time applications (VOIP, bandwidth-hungry live video) and non-real-time applications (audio file transfers, recorded video) can use the same channel at the same time.

Broadband is useful for connectivity by multiple devices spread throughout the whole wide world. Bringing broadband into the public safety workspace is a great idea because cyberspace is a fact of life.

Contrary to the FCC's assumption, there is no technical or administrative way to prevent broadband – especially not wireless broadband – from permeating and being permeated by alien devices. A segmentation of the spectrum makes no difference to security or privacy and a dedicated broadband spectrum exclusively reserved for "eligible local, state, and federal public safety agencies" will not bring all the benefits the FCC intends in paragraphs 12 and 19 of its 9th NPRM.

In short, broadband accessible by "eligible local, state and federal public safety agencies" only is not a tool that can help law enforcement or emergency management.

## 3.6 Recommendation: Exempt essential broadband from licensing

In a disaster it does not matter ***who*** you are, only ***where*** you are. The FCC must therefore:

- view public safety's new dimension, namely emergency management,
- draw a clear distinction between information-sharing and communication,
- recognise that in a disaster, the construction of meaning is begun by those most affected by what is happening, not by eligible agencies only, and
- significantly expand the broadband that already exists.

The FCC will then have the option to propose ***licence-exempt*** broadband, which would in no way conflict with subparagraph (f)(1)(C) of Section 337 of the Communications Act.

In any event, no law which impedes mutual aid should be passed or upheld.

# 4 Methods of communicating for the safety of the public

The FCC's states repeatedly that "[a] key element of permitting commercial service is a strict requirement that any commercial use be unconditionally preemptible by the national public safety licensee." This requirement is dangerously misleading because it is both logically and technically impossible to put into effect.

Public safety uses:

- ***alerts*** with inculcated meanings,
- ***voice*** to extend meaning, to simplify form and to ease understanding, and
- ***broadband***, if available, to gather information quickly so new meaning can be constructed.

No policy to advance broadband is adequate unless it acknowledges the nature of cyberspace and keeps public safety's alerts and voice separate and independent from cyberspace.

Terrorism induces the fear of mass-casualty disasters and so, since September 2001, government entities (as well as specialist defenders against chemical, biological, radiological and nuclear disasters) are being urged, like never before, to acquire interoperability. This is a gigantic cyberspace undertaking. Hooking the communication of all officially recognised organisations together means more and more eggs in fewer and fewer baskets. Doing it in cyberspace is dropping the basket.

Regrettably, the FCC has set its priority as "***reliable*** and interoperable communications (sic)" (Paragraph 1) / "***reliable***, interoperable and broadband communications (sic)" (Appendix, paragraphs 2 and 4, emphasis added) - but the very nature of cyberspace makes this priority an oxymoron. It is crucial that proposals for the safety of the public are judicious about the nature of cyberspace.

The FCC wants to shelter the communication of officially recognised organisations in public safety with a specific band accessible to them only. This endorses the illusion that it is technically possible to keep the uninvited out.

Even if it *were* possible, such a restriction would impede good emergency management and hinder the association so desperately needed in public safety, because it would exclude significant help from all types of organisations and people. In a disaster, the information of a victim or of a passer-by can be as vital as anybody else's (see Dynes 1994).

## 4.1 The three technical approaches to sending information

### 4.1.1 Case 1 - The broadcasting approach

The social need for information is insatiable. It is partly met by broadcasting information through a medium.

In a major emergency it is essential to be able to inform and warn the public. TV and radio are entertainment broadcast media that can readily be used to support and direct the community response to an emergency.

The broadcasting approach uses diverse media.

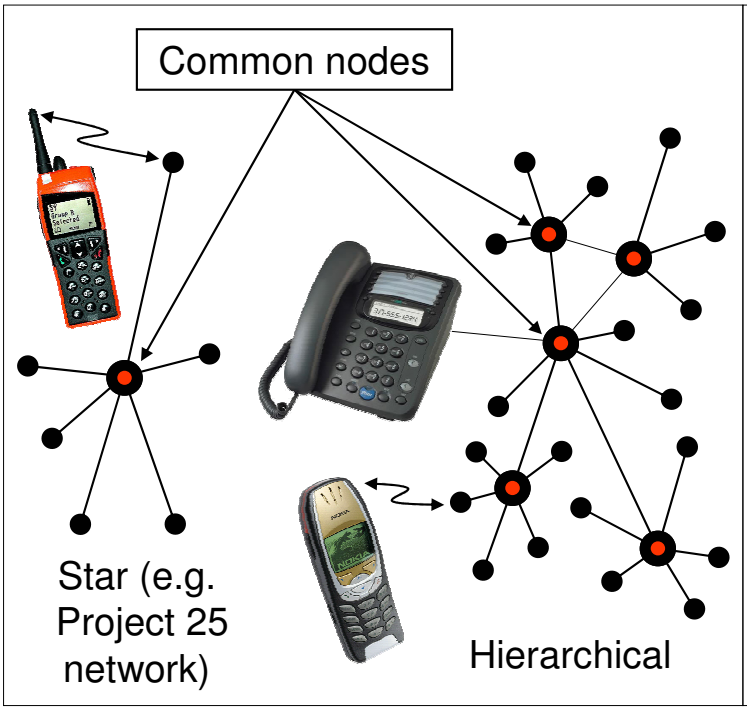
- TV and radio are used to inform and warn the public.
- Sirens are used to give advance warning.
- Radiopaging alerts specific groups.

Sirens give advance warning and then follow-up messages and safety advice are broadcast.

Radiopaging on the other hand, is distinctive and vital for leveraging the readiness of specific groups.

### 4.1.2 Case 2 - The purpose-built, common node approach

Case 2 telecommunication signals are dumb and cannot find their own way. To get to their destinations they are guided by common nodes in a conglomerate of hierarchical networks for mobile phones, telephones and Project 25 radios.




A star network dies if its common node breaks down.

In a hierarchical network, the destruction of only a few common nodes suffices to make telecommunication impossible.

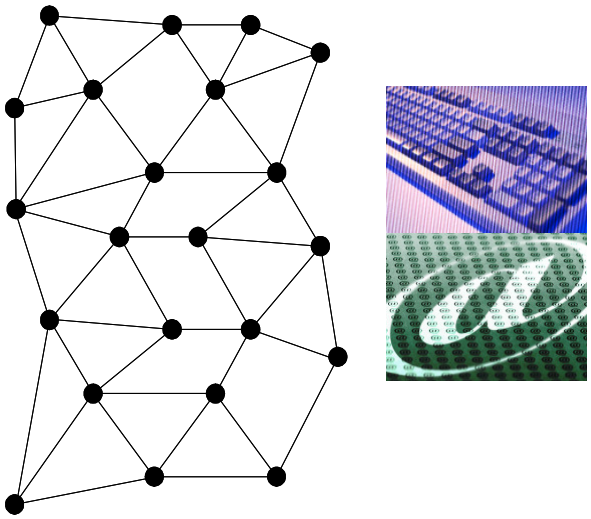
Until the late 1990s, working with dumb signals was acceptable, but now it is not. Technology has become snazzier and uses information that can find its own way. Now no node has command and control over the paths or the veracity of the information.

### 4.1.3 Case 3 - The demand-guided approach

In the 1960s, the USA and the Union of Soviet Socialist Republics (USSR) were gripped by fear of nuclear attack. The US Air Force wanted a telecommunication network that could command a counter-attack.

At that time, significant telecommunication networks were either star or hierarchical, and designed using the common node approach.

According to Paul Baran of the RAND Corporation, the solution lay in building a 'distributed' network which would allow many nodes to communicate by circumnavigating any parts destroyed by enemy attack. This was achieved with packet-switching.



In a distributed network, malfunctioning nodes are circumnavigated by self-guiding information packets.

**Distributed network (from Baran) now called *Cyberspace***

## 4.2 Towards independence from nodes

In the 1980s the US Department of Defence wanted to have interoperability between its sections (air force, navy, army, etc.). It had to choose either to design a unified network capable of providing both fixed and mobile services or else to interconnect the diverse networks which already existed.

A unified network might have yielded compatibility from A to Z, but it soon became clear that it was simply not practical to build from scratch. The grand goal was set to connect the existing networks using the IP packet format already successfully used in the ARPANet during the 1970s.

Researchers worked and worked and worked… and as the research community grew the know-how spread beyond the military. In 1991, IP was officially made available to the public.

IP quickly dominated all other protocols for packet-switching simply because it enables data to be passed from an arbitrary device to an arbitrary device via an arbitrary network. It works for everybody because it enables users to connect different types of computers and eliminates the dependence upon common nodes within the network.

## 4.3 This is cyberspace!

Cyberspace is the fusion of information processing with broadband connectivity. It is the environment in which information is processed and transferred.

The demand for go-as-you-please connectivity has blown away the concept of the pay-as-you-go services. The notion that a network can be built, and that it should ensure circuits, monitor access and measure traffic for call-by-call charging is outdated.

The telephone service used to have prime value, but connectivity is already here - and is what the future is all about. Connectivity is more valuable than any telecommunication service or any individual application such as e-mail or the world-wide web.

Cyberspace includes human interaction and extra-human (device-to-device) interaction. There is new information and there are innumerable new connections and disconnections each day. Cyberspace is, therefore, immeasurable and beyond the control of any person, organisation or country. Likewise power outages, nuclear energy and synthetic chemicals hazards are borderless, and potentially huge.

Unfortunately, cyberspace also allows for miscommunication with every point on the globe. Worse, it indifferently mingles the information of the invited (allies) and of the uninvited (enemies).

## 4.4 What is a cyberspace disruption?

A cyberspace disruption can occur wherever the interacting people or content are corrupt or used maliciously.

Cyberspace disruptions can originate anywhere and cause severe blockages right where you are.

No authority, also not the FCC, can make watertight policy to safeguard against a cyberspace disruption. No amount of legislation, also not the rules proposed in the 9th NPRM, nor any amount of security engineering can safeguard equipment connected to cyberspace.

The paths of interoperable equipment run through countless cyberspace components and any of these can be a point of failure. It is therefore hazardous to rely on

interoperable equipment, especially on Project 25 with its few common nodes, to send warnings or to provide vital voice connections.

| What is at risk in cyberspace? (Case 2 & Case 3 in Sections 4.1.2 & 4.1.3) |
|---|
| **People and property** |
| • Life |
| • Identity |
| • Privacy |
| • Content |
| • Information system configuration data |
| **and infrastructure services** |
| • Communication network configuration data |
| • Vital mediation servers (e.g. network address translators, mobile telephone location area register, etc.) |
| • Capacity (e.g. addressing, bandwidth, throughput rate, memory) |
| • Interoperability / compatibility |
| • Relationships between ends if transferred data arrives changed (End-to-end transparency) |

## 4.5 Is there any certain precaution against the hazards of cyberspace?

- A ***hazard*** is something that has potential to cause harm.
- A ***risk*** is the chance, high or low, of that harm occurring.
- A ***precaution*** is a measure taken, in advance, to lower the risk of harm.

Antivirus software, sensible concealment of passwords, etc. are necessary precautions in cyberspace but it is hard to tell what such 'security measures' actually do and in any event they neither reduce the risk to zero nor eliminate the hazards. After all:

1. Anyone can come in: a door is always open to the invited and uninvited.
2. You don't know if the information is correct: it may be corrupted by error or malice.
3. You don't know who's in charge: cyberspace is spread over a huge number of autonomous authorities and individuals.

4. You can't know where it went wrong: there is no identifiable point of control.

5. You can't check that it all works: there are far too many components, users and uses.

6. You can't fathom what's going on: people, content, connections, technology, instructions, etc. change all the time.

In short, ***no***, there is no certain precaution against the hazards of cyberspace. The only certain way to avoid the hazards of cyberspace is to keep right out of it. This must be applied to vital alerts and to vital voice connections (e.g. for fireground communication) It is simple to do, and inexpensive.

## 4.6 Recommendation: Recognise the hazards of cyberspace

Swissphone recommends that the FCC:

1. accept that wireless broadband is a commodity for everyone,
2. abandon its plan to reserve a segment for eligible agencies only since broadband gizmos permeate and are permeated by cyberspace, and
3. much more boldly acknowledge and warn against the hazards of relying on interoperability especially when, like Project 25, it depends on relatively few common nodes,

# 5 The safety rules of warning

## 5.1 Weight of sent information

In the absence of any certain precaution against the hazards of cyberspace, weighty information should not be exposed to the risk of being abstracted by the technology. Broadband however, can certainly affect the validity of information.

Kenneth Boulding observed:

> *The bit...abstracts completely from the content of information...and while it is enormously useful for telephone engineers...for purposes of the social system theorist we need a measure which takes account of significance and which would weight, for instance, the gossip of a teenager rather low and the communications over the hot line between Moscow and Washington rather high.*
>
> [Frank Webster – *Theories of the Information Society*, Second Edition, Routledge, 2002, pp 25]

A warning facility must quickly and accurately measure the weight of the information about a road accident as low, and that of a nuclear accident as high.

More crucially than voice and broadband, emergency managers and law enforcement agents need - and with radiopaging some do indeed have – an alerting facility that can make such distinctions and broadcast the appropriate signals.

However, in a crisis, it can be extremely difficult to connect, especially when the usual path of communication is busy, congested, or simply knocked out of service.

Anyone attempting a call using two-way systems (telephone, GSM, Project 25 radios) must hope that the call gets through, will be noticed and understood.

## 5.2 Vital warnings

Vital warnings must:

1. impart meaning instantly,
2. use basic technology that is easily kept safe from abuse and deception, and
3. work even when the network-of-networks fails.

### 5.2.1 Meaning and the lack of meaning

Meaning is intelligible if it can be apprehended by the understanding (not by the senses). To inform literally means 'to give form' and so sent information must be reconstructed.

Clear warnings can fail to be understood. For example, investigators of an MD-82 plane crash found that the ground proximity alarm had worked 'perfectly'. But the last words of the Chinese pilot on the cockpit voice recorder were: "What does '*pull up*' mean?" Reconstruction of meaning did not occur and this was fatal.

The meaning of any signal used to alert must be instantly clear to the recipient, because it was inculcated through training.

### 5.2.2 Reducing the risk of miscommunicating warnings

Warnings that are broadcast reduce the risk of miscommunication because they are *one-way*, *end-to-end* (e2e) and *independent*:

***One-way*** transmission prevents attack by an outsider and keeps the ends safe.

***End-to-end*** is an intrinsic characteristic of stand alone transmitters used to alert and to relay alerts (see Section 5.2.3).

***Independent*** means transmission takes place independently of the receivers.

- Messages to alert are passed regardless of the state or whereabouts of the receivers.
- Adding more receivers does not deplete the resources (power, time) of the transmitter.

The communication processes of a Project 25 network are not independent: If too many mobiles call or are called simultaneously, the network becomes congested and

calls are blocked from getting through.

| A one-way path is safer than a two-way path. | | |
|---|---|---|
| | One-way path | Two-way path |
| Type of approach to sending vital information | Case 1 | Case 2 & 3 |
| • Guaranteed anonymity | Yes | No |
| • Authentication | Certain | Uncertain |
| • Monitoring of communication (e.g. legal interception / safe from eavesdropping) | Complete | Incomplete |
| • Access rights (use by intended parties only) | Secure | Not secure |
| • Protection against falsification | Strong | Weak |
| • Protection from use of missing devices (handy, laptop, pager) | Not required | None |
| • Protection from attacks (viruses, denial of service attack) | Robust | Flimsy |
| • Protection from congestion / blocking | Simple | Complex |

### 5.2.3 Loss of network and the illusion that ends are safe

Any network, no matter how carefully designed, will fail to transmit at some time or other.

In a life-and-death situation, a blip in the underlying telecommunication infrastructure must not impede communication. Vital information simply must not be sent relying on any means which depend on the underlying network or a common node.

Saltzer, Reed and Clark (1983), computer scientists of the Massachusetts Institute of Technology provide a reasoning tool e2e (the 'end-to-end arguments') against vulnerability to transmission impairments of all kinds. They argue:

1. A function can be completely and correctly carried out only with the help of the application at the end points.
2. It is wasteful for a network to replicate any function that the end nodes perform anyway.

The first e2e is used to take the competence for the transmission of information away from the network and assign it fully to the ends. However, the competence of the ends is not always correctly assessed.

A new car was designed using incorrect reasoning about the competence of the ends. It was built to activate the airbags and unlock the doors if the car crashed. The hitch with this design was that the ends could not be kept safe. The end - the bumper - was incompetent to recognise abuse. Thieves simply kicked the bumper, and immediately the doors unlocked! The entire series of cars had to be recalled by the manufacturer.

Likewise, in broadband it is impossible to know the competence of the ends. For example, no one can tell what the 'nice young terrorist from next door' is up to. It must never be assumed that an interoperable end always collaborates loyally with other ends.

The ends of a two-way connection path are not safe from each other because, at the very least, they are vulnerable to misunderstanding and to carelessness by one or both ends.

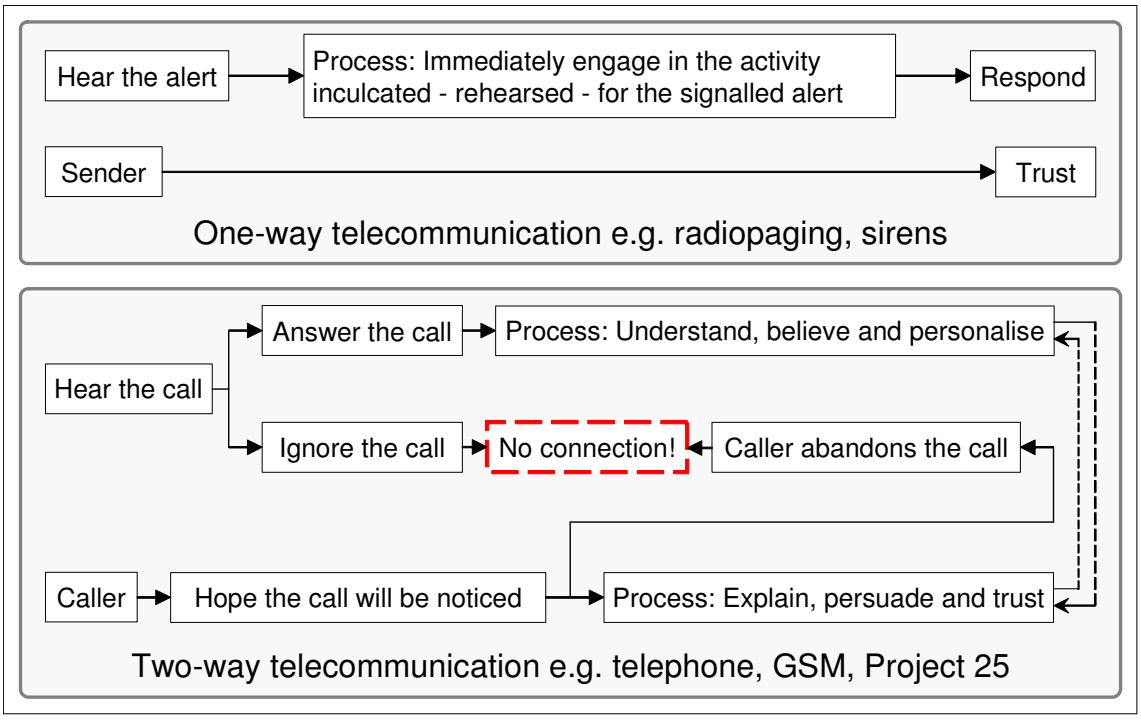
No rules, engineering or security measures can make broadband safe. There is always a risk of deception, attack by a participant, congestion and the loss of network. Protective measures can fail because an insider is negligent or vengeful. In the hands of the wrong person, a two-way communication terminal compromises integrity.

## 5.3 Radiopaging

All methods of sending information to public safety insiders use interoperability - with the exception of radiopaging and end-to-end voice (walkie-talkies).

Radiopaging is omni-directional and increases the likelihood of commands being understood instantly. Radiopaging is the only tool that combines broadcasting, addressing and inculcated meaning and so it is ideal for simple, quick and discreet alerts.

Radiopaging, properly implemented, gives the sender the assurance that every alert is received instantly by more than one receiver and therefore that the alert is noticed. Users of radiopaging are trained to use it to send the right signals. The alert is effective because the sender and receivers using radiopaging immediately understand its meaning, which was inculcated before it was ever used.




**Superiority of radiopaging over two-way systems**

## 5.4 Recommendation: Follow a sound warning doctrine

Swissphone recommends that the FCC:

1. not invest energy in the vain attempt to identify risks and hazards but instead secure what is safe, namely one-way, separate, independent communication processes (2. and 3. below),
2. keep enough HF, VHF and UHF frequencies for simplex or semi-duplex 'push-to-talk' analogue radios (end-to-end walkie-talkies),
3. keep enough HF, VHF and UHF frequencies to warn with one-way, end-to-end, radiopaging, and
4. guard the frequencies of local media broadcasters (TV and radio) that can support and direct the community response,

guided by the imperative to protect life and property rather than an 'efficient' use of the spectrum.

# 6 Comments for spectrum utilisation - *ad hoc* broadband

Swissphone's detailed comments on the FCC's *9th NPRM* on a centralised approach to the *Implementation of a Nationwide, Broadband, Interoperable Public Safety Network in the 700MHz Band* (PS Docket No. 06-229 and WT Docket No. 96-86), available at: http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-06-181A1.doc

| 9th NPRM section/§ | Issue presented by the FCC (without footnotes) | Swissphone's comment |
|---|---|---|
| ***I INTRODUCTION*** | | |
| 1 | *In the Commission's Eighth Notice of Proposed Rulemaking, the Commission sought comment on whether certain channels within the current 24 megahertz of public safety spectrum in the 700 MHz band (764-776 MHz and 794-806 MHz) should be modified to accommodate broadband communications. The Commission stated that this action "is consistent with national priorities focusing on homeland security and broadband and our commitment to ensure that emergency first responders have access to reliable and interoperable communications".* | The focus on broadband is welcomed.<br><br>To get a fine, sharp image of the three national priorities the FCC has set, it is really, really important to use disaster research to recognise the communication needs of all types of organisations involved in mutual aid (Section 1.2).<br><br>Moreover, the FCC must have a sound doctrine about how warnings are produced, verified and issued (Section 3.4). |

| 9th NPRM section/§ | Issue presented by the FCC (without footnotes) | Swissphone's comment |
|---|---|---|
| 2 | *As also noted in the Eighth NPRM, the Commission previously announced principles for ensuring effective public safety use of the 700 MHz band, including standardization necessary to achieve nationwide interoperability, development of competitive equipment markets, and a degree of regional flexibility necessary to allow opportunities for tailored approaches to meeting the needs of regional communities. The Commission also noted that Congress has recognized that the 700 MHz spectrum is "ideal" for providing first responders with interoperable communications channels, and established February 17, 2009 as the date by which this spectrum will be cleared of incumbent broadcasters. Furthermore, the Commission found, in its Report to Congress submitted pursuant to the Intelligence Reform Act, that deployment of an integrated, nationwide, interoperable network capable of delivering broadband communications would offer the public safety community many benefits, including video surveillance, real-time text messaging and email, high resolution digital images and the ability to obtain location and status information of personnel and equipment in the field. We thus are presented with an opportunity to put into place a regulatory framework that would ensure the availability of effective spectrum in the 700 MHz band for interoperable, public safety use.* | The aim of building large-scale, purpose-built networks is completely outdated. It does not excite investors and it does not stimulate the producers of snazzy micro-chips.<br><br>"First responders with interoperable communications channels":<br>1. hazardously rely on interoperable equipment with its few, vulnerable common nodes (Section 4.4).<br>2. are excluded from telecommunication with other organisations (Disaster Research Center (DRC) Type II, III and IV) who are often first on the scene (Section 1.2.1). |

| 9th NPRM section/§ | Issue presented by the FCC (without footnotes) | Swissphone's comment |
|---|---|---|
| 3 | *In this Ninth Notice of Proposed Rulemaking, we seek to expand and build upon the themes raised in the Eighth NPRM by proposing a comprehensive plan that we believe may best promote the rapid deployment of a nationwide, interoperable, broadband public safety network, and thereby improve emergency responsiveness. Particularly in light of the nation's current and anticipated public safety and homeland security needs, we propose a centralized and national approach to maximize public safety access to interoperable, broadband spectrum in the 700 MHz band, and, at the same time, foster and promote the development and deployment of advanced broadband applications, related radio technologies, and a modern, IP-based system architecture.* | Yeah to broadband - on condition that spectrum:<br>1. is not fragmented,<br>2. ports broadband ports to where events outpace so-called first responders with only uplinks and downlinks to fixed transponders, and<br>3. accommodates everyone (Section 2). |

| 9th NPRM section/§ | Issue presented by the FCC (without footnotes) | Swissphone's comment |
|---|---|---|
| 4 | *Our proposed plan is a departure from prior public safety allocations, and is designed to speed deployment, decrease costs of roll-out, promote nationwide interoperability and provide a source of funding for constructing a broadband public safety communications network. The proposal includes that the Commission (1) allocate 12 megahertz of the 700 MHz public safety spectrum from wideband to broadband use; (2) assign this spectrum nationwide to a single national public safety broadband licensee; (3) permit the national public safety broadband licensee also to operate on a secondary basis on all other public safety spectrum in the 700 MHz band; (4) permit the licensee to use its assigned spectrum to provide public safety entities with public safety broadband service on a fee for service basis; (5) permit the licensee to provide unconditionally preemptible access to its assigned spectrum to commercial service providers on a secondary basis; (6) facilitate the shared use of commercial mobile radio service (CMRS) infrastructure for the efficient provision of public safety broadband service; and (7) establish performance requirements for interoperability, build out, preemptibility of commercial access, and system robustness.* | The FCC's states repeatedly that "[a] key element of permitting commercial service is a strict requirement that any commercial use be unconditionally preemptible by the national public safety licensee." This requirement is dangerously misleading because it is both logically and technically impossible to put into effect, let alone to measure without a huge crisis (Section 4).<br><br>Even if it *were* possible, such a restriction would impede good emergency management and hinder the association so desperately needed in public safety, because it would exclude significant help from all types of organisations and people. In a disaster, the information of a victim or of a passer-by can be as vital as anybody else's (see Dynes Russell R. 1994. *Community emergency planning: False assumptions and inappropriate analogies*. Disaster Research Center, University of Delaware, available at http://dspace.udel.edu). |

| 9th NPRM section/§ | Issue presented by the FCC (without footnotes) | Swissphone's comment |
|---|---|---|
| ***II BACKGROUND*** | | |
| 7 | *The Commission has made progress towards achieving nationwide interoperability in the 700 MHz public safety band. In 2000, the Public Safety National Coordination Committee (NCC) recommended that the Commission adopt Project 25 Phase I (Project 25) as the interoperability standard for the narrowband interoperability channels. Subsequently, the Commission adopted Project 25 as the narrowband digital standard for the interoperability channels. As a result, mobile and portable narrowband radios are required to be capable of operating on the interoperability channels using the Project 25 standard, ensuring that all public safety entities using 700 MHz narrowband radios will be able to communicate with each other. Thus, the Commission and the public safety community are poised to move forward with nationwide interoperability on the narrowband channels, once this spectrum is cleared of incumbent broadcasters.* | Disaster research shows that even where interoperable radios were available, government agencies could not communicate.<br><br>The way to progress is to facilitate mutual aid by using everyone's broadband instead of aiming at the 'standardisation' of limited means for established organisations (DRC Type I) only (Section 3.5).<br><br>Project 25 is, at best, adequate for day-to-day work but has proved lamentably unsuitable for mutual aid.<br><br>The Commission ought to reflect on the history of radio regulation as it relates to disasters. Before asking people to use the spectrum 'efficiently', the FCC has the duty to protect life and property.<br><br>The "public safety community" has been transformed. The FCC must consider everyone who is involved and the ***most basic means*** of communication used to share information in life-and-death situations (i.e. voice and warnings) - see Section 3.1 and Worrell, Mike and MacFarlane, Andy, 2004. *Phoenix Fire Department Radio System Safety Project*, Final Report, available at: http://www.phoenix.gov/FIRE/radioreport.pdf |

| 9th NPRM section/§ | Issue presented by the FCC (without footnotes) | Swissphone's comment |
|---|---|---|
| ***III DISCUSSION*** | | |
| ***A. Objectives of Public Safety Model*** | | |
| 12 | ***Broadband.*** *Presently, there is no allocation in the 700 MHz public safety band for broadband communications. Broadband technologies hold the potential to provide public safety entities integrated access to voice and high-speed data capabilities, and thus may dramatically reduce the time it takes to access information during emergencies. We believe that we should maximize opportunities for broadband use of 700 MHz spectrum due to the many benefits of broadband communications, including video surveillance, real-time text messaging and email, high resolution digital images and the ability to obtain location and status information of personnel and equipment in the field. For example, police officers could exchange mug shots, fingerprints, photographic identification, and enforcement records; firefighters could have access to floor and building plans and real-time medical information; forensic experts could provide high resolution photographs of crime scenes and real-time video monitoring transmitted to incident command centers.* | A segmentation of the spectrum makes no difference to security or privacy and a dedicated broadband spectrum exclusively reserved for "eligible local, state, and federal public safety agencies" will not bring all the benefits the FCC intends in paragraphs 12 and 19 of its 9th NPRM.<br><br>In short, broadband accessible by "eligible local, state and federal public safety agencies" only is not a tool that can help law enforcement or emergency management (Section 3.5). |

| 9th NPRM section/§ | Issue presented by the FCC (without footnotes) | Swissphone's comment |
|---|---|---|
| 13 | ***Nationwide Interoperability.*** *All emergency personnel involved in an incident need to be able to communicate seamlessly. The availability of a nationwide, interoperable, broadband communications network for public safety substantially could enhance the ability of public safety entities to respond to emergency situations, whether due to severe weather events or criminal or terrorist activities, and likely would save lives and preserve property. Yet, only 2.6 megahertz is designated for nationwide interoperable communications in the 700 MHz public safety band. Furthermore, the radios used by federal, state and local first responders generally are not interoperable. Instead, the highly fragmented structure of public safety agencies, whether among different public safety agencies serving the same community (i.e., local police, fire, emergency medical), neighboring communities or states, or among local, state, and federal levels, has resulted in many different and distinct communications infrastructures. As a consequence, public safety personnel often must carry multiple radios to coordinate their activities. Even when some interoperability is reached on a regional level, there still is a lack of nationwide interoperability.* | This state of affairs came about through rule-making that was inconsistent with mutual aid.<br><br>St. Luke Chapter 10:25-37 is the bedrock of public safety on which the Wireless Ship Act of June 24, 1910, was built. With these as its context, the FCC ought to do everything in its power to accommodate everyone's broadband in mutual aid. |

| 9th NPRM section/§ | Issue presented by the FCC (without footnotes) | Swissphone's comment |
|---|---|---|
| 14 | ***Adequate Funding.*** *Any proposal for improving public safety communications should address potential new sources of funding. Traditionally, public safety agencies have had great difficulty funding the build-out and operation of modern communications systems. None of the other objectives of a public safety communications system can be met without adequate funding.* | Manufacturers of broadband are consumer-market driven – specifically, digital media products. For example, Infineon states that the volume of ICs it manufactures for consumer products today exceeds the volume it manufactures for the IT and government markets combined.<br><br>If the FCC restricts broadband to a minority with an insignificant and unpalatable monopsony, the industry will be unwilling and the difficulty of funding will be exacerbated.<br><br>By making broadband ***license-exempt***, the FCC will stimulate the industry and funding for building a new, large-scale, purpose-built network will become unnecessary. |

| 9th NPRM section/§ | Issue presented by the FCC (without footnotes) | Swissphone's comment |
|---|---|---|
| 16 | ***Efficient Spectrum Use.*** *Public safety communications systems should be spectrum-efficient. Public safety services should use spectrum efficient technologies that appropriately reflect the value of spectrum. For example, public safety providers could increase capacity through improvements in infrastructure when it is less costly than adding spectrum. The high spectrum efficiency observed in the production of CMRS could be a benchmark for public safety.* | Spectrum is efficient if it can be used where people converge. The best way to make spectrum efficient is to let broadband devices build the network themselves, quickly, and as they go along.<br><br>Already *ad hoc* broadband is used for connectivity which:<br><br>1. makes short and long range hops,<br>2. decreases the information throughput whenever it is necessary to increase range, and<br>3. carries transit or terminating/originating traffic and not just uplink and downlink traffic.<br><br>See:<br><br>Toumpis, Stavros, 2005. Topics *on Wireless Ad Hoc Networks – Overview*, Tele-communications Research Center Vienna, available at: http://www.eng.ucy.ac.cy/toumpis/courses/ad_hoc/overview.pdf<br><br>Toumpis, Stavros, 2005. *Topics on Wireless Ad Hoc Networks – Capacity of Large Networks with Immobile Nodes*, Tele-communications Research Center Vienna, available at: Capacity.pdf |

| 9th NPRM section/§ | Issue presented by the FCC (without footnotes) | Swissphone's comment |
|---|---|---|
| 17 | ***Robustness.*** *Survivability is an important objective of the envisioned nationwide public safety broadband system. The widespread destruction caused by Hurricane Katrina illustrated the vulnerability of the terrestrial communications infrastructure to natural disasters, as well as similarly destructive terrorist attacks. When a disaster destroys the terrestrial infrastructure, public safety workers can be left without any communications. The system could be inherently robust by incorporating flexible routing and other features (possibly including a satellite component operating in other spectrum) that will maintain essential operations when parts of the infrastructure have been destroyed or disabled.* | ***License-exempt***, *ad hoc* broadband means that gizmos, we know not from where, actually make the network by themselves, quickly, and as they go along. They allow for the happenstance of sharing vital information on mutual aid occasions.<br><br>*Ad hoc* broadband does not depend on any common node. |

| 9th NPRM section/§ | Issue presented by the FCC (without footnotes) | Swissphone's comment |
|---|---|---|
| ***B. Proposal*** | | |
| 19 | *We propose that the 12 megahertz of spectrum at 767-773 MHz and 797-803 MHz, currently designated as wideband segments, be allocated for broadband use and that a single, national public safety broadband licensee be assigned this spectrum on a primary basis. The licensee also would be authorized to use all other public safety spectrum in the 700 MHz band on a secondary basis. Using this spectrum, the licensee would be authorized to provide public safety agencies voluntary access to broadband services, on a fee-for-service basis. The licensee also would be permitted to provide unconditionally preemptible access to this spectrum to commercial entities through leases or in the form of public/private partnerships. The national public safety broadband licensee may enter into arrangements with commercial service providers for accessing or sharing their communications systems infrastructure in order to create the nationwide, interoperable, broadband public safety communications network. We would leave significant discretion to the national licensee to carry out its responsibilities. We believe, however, that it would be necessary for the Commission to establish certain baseline performance requirements, including those for broadband, interoperability, build-out of national coverage, unconditional preemption of commercial use, and disaster restoration capability. We seek comment broadly on our proposed approach or any alternatives, as well as any potential impact on existing operations or planning activities by public safety in this spectrum.* | It is dangerously misleading of the FCC to require or permit preemptible access, and to purport that it could possibly be beneficial to exclude any kind of user in mutual aid (Section 4).<br><br>The Wireless Ship Act of 1910 did not require that radio be for the coast guard only.<br><br>**Alternative**<br><br>Methods of communication with *ad hoc* broadband, consistent with what disaster researchers call '*emergence*' and '*convergence*', are described in:<br><br>Toumpis, Stavros, 2005. *Topics on Wireless Ad Hoc Networks – Overview*, Telecommunications Research Center Vienna, available at: http://www.eng.ucy.ac.cy/toumpis/courses/ad_hoc/overview.pdf<br><br>Toumpis, Stavros, 2005. *Topics on Wireless Ad Hoc Networks – Capacity of Large Networks with Immobile Nodes*, Tele-communications Research Center Vienna, available at: Capacity.pdf<br><br>Channels that rely on a few common nodes are acceptable for casual, day-to-day work but not for mutual aid.<br>For mutual aid, broadcast, end-to-end, communication (Section 5.4) and multi-media broadband (Section 3.6) are indispensable. |

| 9th NPRM section/§ | Issue presented by the FCC (without footnotes) | Swissphone's comment |
|---|---|---|
| ***1. Single National Public Safety License*** | | |
| 20 | *A central theme of our proposal is the licensing of a single, national public safety entity for the provision of public safety broadband service in lieu of the traditional practice of licensing individual state and local jurisdictions. We believe that centralizing the licensee responsibilities into a single entity representative of the public safety community could best serve the objectives discussed above. A centralized, national network providing a wide range of communications services on a broadband backbone, using a flexible, modern architecture, could (1) enable nationwide interoperability; (2) reduce costs; (3) increase efficiency of spectrum usage; and (4) enhance network robustness.* | If the FCC is concerned with keeping the public safe, the central theme ought to be exemption of broadband for mutual aid from licensing by the FCC.<br><br>N.B. The safety of the public is everybody's business. It is not the exclusive domain of officially recognised organisations, nor even of homeland security (Sections 1 and 2). |

| 9th NPRM section/§ | Issue presented by the FCC (without footnotes) | Swissphone's comment |
|---|---|---|
| 21 | ***Interoperability.*** *A national public safety licensee may be in the best position to solve the interoperability and broadband capacity problems that have been the topic of increased concern, especially apparent in the wake of 9/11 and last year's hurricanes. A single, national network could provide a nationwide level of interoperability not achievable by an otherwise fragmented approach. A centralized approach also could ensure a single technical framework for system implementation that could be designed, for example, to provide adequate capacity for new high-bandwidth uses including real-time mobile video.* | Interoperability is, in itself, a topic of increasing controversy because it has failed. See two examples:<br><br>Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks, *Report and Recommendations to the Federal Communications Commission*, June 12, 2006, available at: http://www.fcc.gov/eb/hkip/karrp.pdf<br><br>Oral Testimony of Commissioner Steven M. Gregory, Federal Communication Commission Public Safety National Coordinating Committee, General Membership Meeting, Transcript at pp. 41-53 (Friday, November 16, 2001) available at:<br>November 16, 2001 General Membership Meeting Transcript<br><br>Two examples are not enough to make rules, but the body of disaster research is. See Section 1 of the Bibliography.<br><br>Words like 'interoperability' ***45***, 'reliable' ***6*** and 'system' ***72*** have lost their meaning or now have simultaneous, contradictory meanings (numbers written in ***bold italics*** indicate the number of times each respective word is used in FCC 06-181, Released: Dec. 20, 2006). |

## Interoperability in misleading terminology and in sane English

Interoperability is generally thought to mean unproblematic and even effortless communication between various responders. It is, however, not merely a technical problem which can be solved with purpose-built stuff that has an availability of more than 99.999%.

Because of their mutual interactions, human activity and extra-human (device-to-device) activity cannot be considered in isolation.

| 'Interoperability' in misleading terminology - ITU-T Rec. X.901, pp. 7, 1997 | 'Interoperability' in sane English (Section 4.5) |
|---|---|
| *In order both to manage system distribution and to exploit it (e.g. use the potential for availability, performance, dependability and cost optimization), organizations must deal with a number of key characteristics of system distribution.* | **There is no one in control**: the ownership of the machine is distributed. |
| ***Lack of global state**: The global state of a distributed system cannot be precisely determined.* | **You can't check that it all works**: there are far too many components, users and uses. |
| ***Partial failures**: Any component of a distributed system may fail independently of any other component.* | **You can't know where it goes wrong**: there is no identifiable point of control. |
| ***Autonomy**: A distributed system can be spread over a number of autonomous management or control authorities, with no single point of control. The degree of autonomy specifies the extent to which processing resources and associated devices (printers, storage devices, graphical displays, audio devices, etc.) are under the control of separate organizational entities* | **You don't know who's in charge:** cyberspace is spread over a huge number of autonomous authorities and individuals. |
| ***Mobility**: The sources of information, processing nodes, and users may be physically mobile. Programs and data may also be moved between nodes, e.g. in order to cope with physical mobility or to optimize performance.* | **You can't fathom what's going on**: people, content, connections, technology, instructions, etc. change all the time. |

With interoperability being what it is (sane English), it is imperative that warnings can be broadcast by one-way communication systems (walkie-talkies, radiopaging, TV, radio, sirens etc.) that are kept separate and independent from cyberspace.

| 9th NPRM section/§ | Issue presented by the FCC (without footnotes) | Swissphone's comment |
|---|---|---|
| 26 | ***Robustness and survivability.*** *Finally, a single national licensee may be in a better position to ensure robustness and survivability, especially when large geographic areas are affected that cut across traditional public safety jurisdictions. A national licensee also may be in a uniquely advantageous position to efficiently stockpile equipment and transportable infrastructure that could be deployed quickly to disaster areas as needed. It also could be well-situated to contract for national satellite service and benefit from economies of scale in integrating satellite capability into its radios to the extent that such integration is beneficial.* | ***License-exempt***, *ad hoc* broadband means that gizmos, we know not from where, actually make the network by themselves, quickly, and as they go along. They allow for the happenstance of sharing vital information on mutual aid occasions.<br><br>*Ad hoc* broadband does not depend on any common node.<br><br>Stockpile: Anyone needing to communicate can go to the nearest shopping mall and buy the broadband gizmo everyone else is working with. There's no way that a single national licensee will be able to operate more efficiently than the commercial distributors. |
| ***4. Requirements of the National Public Safety Network*** | | |
| 31 | ***Broadband Communications.*** *We seek comment on how the national licensee can best implement a broadband network that maximizes the inherent advantages of broadband communications. We do not intend, however, for our proposals herein to preclude our consideration of alternative band plans for the Upper 700 MHz Guard Band spectrum, including the rearrangement of the channels within the public safety allocation.* | The way to maximise the inherent advantages of broadband is:<br>1. not to fragment the spectrum,<br>2. to exempt all the spectrum that can be allocated to broadband for mutual aid, today and in the future, from licensing by the FCC. |

| 9th NPRM section/§ | Issue presented by the FCC (without footnotes) | Swissphone's comment |
|---|---|---|
| 32 | ***System Architecture.*** *Modern IP-based system architecture has many advantages in terms of flexibility and cost. It could enable multiple technologies – narrowband terrestrial, broadband terrestrial and satellite – to be integrated. This could permit the joint use of a common infrastructure by commercial and public safety users, with priority for public safety users. It could provide great flexibility in combining multiple services, e.g., voice, data and video, into the same device. It could allow the public safety system to benefit from economies of scale in the production of commercial devices. On the other hand, there may be issues as to whether IP technology can provide the required quality-of-service guarantees for certain public safety applications that must operate with a high degree of reliability in life-threatening situations. Should the national public safety licensee have the discretion to choose the best system architecture, or should the Commission establish system architecture requirements, and, if so, what should they be?* | Hooking the communication of all officially recognised organisations together means more and more eggs in fewer and fewer baskets. Doing it in cyberspace is dropping the basket (Section 4).<br><br>The FCC must, instead, follow a sound warning doctrine and<br>1. not invest energy in the vain attempt to identify risks and hazards but instead secure what is safe, namely one-way, separate, independent communication processes.<br>2. keep enough HF, VHF and UHF frequencies for simplex or semi-duplex 'push-to-talk' analogue radios (end-to-end walkie-talkies), and<br>3. keep enough HF, VHF and UHF frequencies to warn with one-way, end-to-end, radiopaging (Section 5.4). |

| 9th NPRM section/§ | Issue presented by the FCC (without footnotes) | Swissphone's comment |
|---|---|---|
| 34 | *We also seek comment on whether federal law enforcement and other federal users such as the Department of Defense should be permitted to use the national broadband public safety broadband communications system and, if so, on what basis. Federal users may find subscribing to a nationwide, broadband public safety system to be a cost-effective alternative or complement to the construction of separate systems. Joint use of a common infrastructure by federal, state and local public safety agencies also could facilitate interoperability and coordination between those sectors.* | The FCC wants to shelter the communication of officially recognised organisations in public safety with a specific band accessible to them only, and considers special invitations to other federal users. This endorses the illusion that it is technically possible to keep the uninvited out (Section 4). |

| 9th NPRM section/§ | Issue presented by the FCC (without footnotes) | Swissphone's comment |
|---|---|---|
| 36 | ***Network Resiliency and Disaster Restoration.*** *Public safety communications should be robust against destruction of terrestrial infrastructure. This may require that the national public safety network proposed herein incorporate one or more of the following: IP-based routing, a satellite component (via arrangements with satellite providers), and temporary base stations (on the ground and in aircraft) that can be deployed in emergencies. We seek comment on what requirements, if any, the Commission should establish for network resiliency and disaster restoration and how any such requirements should be specified. Should some robustness requirements be imposed on all public safety systems, not just the national public safety system?* | Network resiliency means people not only technology.<br><br>In times of danger, warnings that are broadcast reduce the risk of miscommunication because they are *one-way*, *end-to-end* (e2e) and *independent*:<br><br>***One-way*** transmission prevents attack by an outsider and keeps the ends safe.<br><br>***End-to-end*** is an intrinsic characteristic of stand alone transmitters used to alert and to relay alerts (see Section 5.2.3).<br><br>***Independent*** means transmission takes place independently of the receivers.<br>• Messages to alert are passed regardless of the state or whereabouts of the receivers.<br>• Adding more receivers does not deplete the resources (power, time) of the transmitter.<br><br>The communication processes of a Project 25 network are not independent: If too many mobiles call or are called simultaneously, the network becomes congested and calls are blocked from getting through.<br><br>(Section 5.2.2) |

| 9th NPRM section/§ | Issue presented by the FCC (without footnotes) | Swissphone's comment |
|---|---|---|
| ***6. Unconditional Preemptible Access to Commercial Service Providers and Joint Provision with Commercial Services*** | | |
| 41 | *Under our proposal, the national public safety licensee would be permitted to lease access to commercial service providers on an unconditionally preemptible basis and enter into spectrum lease arrangements with commercial service providers in the manner of a public/private partnership for joint provision of public safety and commercial services. A key element of permitting commercial service is a strict requirement that any commercial use be unconditionally preemptible by the national public safety licensee. Specifically, commercial users would be on plain notice that their use may be, without notice, subject to immediate termination at the sole discretion of the national public safety licensee. We propose that there would be no conditions placed on the national licensee prior to making a determination to cease secondary commercial use. The national public safety licensee would have the unfettered right, which cannot be compromised or contracted away, to unilaterally determine when a secondary commercial use must be discontinued in the interests of public safety. Clearly, then, commercial users would need to ensure that, as part of any business plan, they have spectrum or communications alternatives in place to anticipate the event that their use may be preempted. We also envision, however, that our dedication to creating a nationwide, interoperable, broadband public safety network could incent accelerated development and use of advanced technologies, such as cognitive radios, by both public safety users as well as secondary commercial users. We seek comment on our proposal to permit commercial use on an unconditional preemptible basis as described above.* | The FCC's states repeatedly that "[a] key element of permitting commercial service is a strict requirement that any commercial use be unconditionally preemptible by the national public safety licensee." This requirement is dangerously misleading because it is both logically and technically impossible to put into effect, let alone to measure without a huge crisis (Section 4).<br><br>Even if it *were* possible, such a restriction would impede good emergency management and hinder the association so desperately needed in public safety, because it would exclude significant help from all types of organisations and people. In a disaster, the information of a victim or of a passer-by can be as vital as anybody else's (see Dynes Russell R. 1994. *Community emergency planning: False assumptions and inappropriate analogies*. Disaster Research Center, University of Delaware, available at http://dspace.udel.edu). |

| 9th NPRM section/§ | Issue presented by the FCC (without footnotes) | Swissphone's comment |
|---|---|---|
| 46 | *We also note that Section 337(a)(1) of the Communications Act requires that the 700 MHz public safety spectrum be allocated for "public safety services," and Section 337(f) defines "public safety services" as follows:*<br>*(f) Definitions. For purposes of this section:*<br>*(1) Public safety services. The term "public safety services" means services –*<br>*(A) the sole or principal purpose of which is to protect the safety of life, health, or property;*<br>*(B) that are provided –*<br>*(i) by State or local government entities; or*<br>*(ii) by nongovernmental organizations that are authorized by a governmental entity whose primary mission is the provision of such services; and*<br>*(C) that are not made commercially available to the public by the provider.*<br><br>*In light of this statutory provision – particularly subparagraph (f)(1)(C) – we seek comment on whether it would be necessary, in order to allow the commercial use of this spectrum on an unconditionally preemptible, secondary basis, to make a specific allocation for such secondary use in the 700 MHz public safety band and then issue a separate license to the national licensee for purposes of offering such use of the network on this basis. If these measures are not statutorily required, we propose to incorporate directly into the national public safety license a license term permitting such commercial use. While we consider the proposal to comport with all statutory requirements, we welcome comment on the issue of whether our proposal is generally consistent with Section 337.* | In a disaster it does not matter ***who*** you are, only ***where*** you are. The FCC must therefore:<br>• view public safety's new dimension, namely emergency management,<br>• draw a clear distinction between information-sharing and communication,<br>• recognise that in a disaster, the construction of meaning is begun by those most affected by what is happening, not by eligible agencies only, and<br>• significantly expand the broadband that already exists.<br><br>The FCC will then have the option to propose ***licence-exempt*** broadband, which would in no way conflict with subparagraph (f)(1)(C) of Section 337 of the Communications Act.<br><br>In any event, no law which impedes mutual aid should be passed or upheld. Consistent with the Wireless Ship Act of June 24, 1910 and successive radio regulations, the FCC ought to boldly uphold what is legitimate in a disaster; not just what is legal and economically optimal in times of 'normalcy'. |

# Bibliography

## 1 On disaster research

Averill, D. et al., 2005. *Federal Building and Fire Safety Investigation of the World Trade Center Disaster – Occupant Behavior, Egress, and Emergency Communications*, Building and Fire Research Laboratory, National Institute of Standards and Technology, September 2005, available at: http://wtc.nist.gov/NISTNCSTAR1-7.pdf

Dynes, Russell R. 1994. *Community emergency planning: False assumptions and inappropriate analogies*. Disaster Research Center, University of Delaware, available at: http://dspace.udel.edu:8080/dspace/bitstream/19716/1626/1/Article%20275.pdf

Federal Communication Commission Public Safety National Coordinating Committee, General Membership Meeting, Friday, November 16, 2001, transcript available at: November 16, 2001 General Membership Meeting Transcript

Kreps, G. A., 1983, *The organisation of disaster response - Core concepts and processes*, International Journal of Mass Emergencies and disasters, 1983, pp 439 – 465, available at: http://www.training.fema.gov/EMIWeb/downloads/IJEMS/ARTICLES

Mileti, D. S. and Sorensen, J. H., 1990, *Communication of Emergency Public Warnings – A Social Science Perspective and State-of-the-Art Assessment*, Oak Ridge National Laboratory, available at: http://emc.ornl.gov/EMCWeb/EMC/PDF/CommunicationFinal.pdf

Quarantelli, E. L., 1990, *Emergency*, Disaster Research Centre, University of Delaware, available at: http://dspace.udel.edu:8080/dspace/bitstream/19716/1328/3/PP%20143.pdf

Quarantelli, E. L., 1999. *Research based criteria for evaluating disaster planning and managing*. Newark, DE: Disaster Research Center, University of Delaware, available at: http://www.udel.edu/DRC/preliminary/246.pdf

Quarantelli, E. L., 2000, *Disaster planning, emergency management and civil protection: the historical development of organised efforts to plan and to respond to disasters*. Disaster Research Centre, University of Delaware, available at: http://dspace.udel.edu:8080/dspace/handle/19716/673

Quarantelli, E.L., 2003. *A Half Century of Social Science Disaster Research: Selected Major Findings and their Applicability*. Disaster Research Center, University of Delaware, 2003, available at: http://dspace.udel.edu:8080/dspace/handle/19716/297

Stallings, Robert A., 1971. *Organizational Change and the Concept of Structure*, Disaster Research Center, University of Delaware, available at: http://dspace.udel.edu:8080/dspace/handle/19716/1185

## 2 On communication

Chandler, Daniel, 1994. *The Transmission Model of Communication*, UWA. Transmission Model of Communication

Mann, Bill. *What is Communication? – A Survey*. http://www-rcf.usc.edu/~billmann/WMlinguistic/cq-sent.pdf

Ortony, Andrew, 1993. *Metaphor and Thought*, Second Edition, Cambridge University Press.

## 3 On the original motif for US radio communication law

Herring, M. James and Gross, C. Gerald, 1936. *Telecommunications: Economics and Regulation*, McGraw-Hill Book Company, Inc, New York.

Maclaurin W. R., 1949. *Invention and Innovation in the Radio Industry*, The MacMillan Company, New York.

## 4 Federal Communications Commission proceedings

Federal Communications Commission Public Safety National Coordinating Committee, General Membership Meeting, Friday, November 16, 2001, transcript available at: November 16, 2001 General Membership Meeting Transcript

Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks, *Report and Recommendations to the Federal Communications Commission*, June 12, 2006, available at: http://www.fcc.gov/eb/hkip/karrp.pdf

## 5 On communication failures that were fatal

Jones, R. Kent, 2003. *Miscommunication between pilots and air traffic control*, Language Problems & Language Planning Volume 27, Number 3, 2003, pp. 233 – 248 (16).

Federal Communication Commission Public Safety National Coordinating Committee, General Membership Meeting, Friday, November 16, 2001, transcript available at: November 16, 2001 General Membership Meeting Transcript

Lawson, Randal and Vettori, Robert, 2005. *Federal Building and Fire Safety Investigation of the World Trade Center Disaster – The Emergency Response Operations*, Building and Fire Research Laboratory, National Institute of Standards and Technology, September 2005, available at: http://wtc.nist.gov/NISTNCSTAR1-8.pdf

Pearson, David E., 2000. *The World Wide Military Command and Control System - Evolution and Effectiveness*, Air University Press, Maxwell Air Force Base, Alabama, June 2000. http://aupress.maxwell.af.mil/Books/Pearson/Pearson.pdf

Weick, Karl, 1993. *The Collapse of Sensemaking in Organisations: The Mann Gulch Disaster*, Administrative Science Quarterly; 38 (1993) pp 628-625 *available at*: http://projects.ischool.washington.edu/ ... weick-mann.gulch.pdf

# 6 On snazzy approaches to broadband

Baran, Paul, 1994. Keynote Talk Transcript, 8th Annual Conference on Next Generation Networks, Washington, DC, November 9, 1994. *Visions of the 21st Century Communications: Is the Shortage of Radio Spectrum for Broadband Networks of the Future a Self Made Problem?* Available at: http://www.dandin.com/pdf/baran1994.pdf

Baran, Paul, 2002. *The Beginnings of Packet Switching: Some Underlying Concepts*, IEEE Communications Magazine, July 2002, available at http://www.csm.ohiou.edu/hoag/baran.pdf

Carpenter, B., 1996. *Architectural Principles of the Internet*, RFC 1958, available at: http://www.ietf.org/rfc/rfc1958.txt

Carpenter, B., 2000. *Internet Transparency*, RFC 2775, available at: http://www.ietf.org/rfc/rfc2775.txt

Clark, David, 1988. *The Design Philosophy of the DARPA Internet Protocols*, Proc SIGCOMM 88, ACM CCR Vol 18, Number 4, August 1988, pp 106 -114 (reprinted in ACM CCR Vol 25, Number 1, January 1995, pp 102 - 111) available at: http://nms.csail.mit.edu/6829-papers/darpa-internet.pdf

Saltzer, J.H., Reed, D.P., Clark, D.D., 1984. *End-To-End Arguments in System Design*, ACM TOCS, Vol 2, Number 4, November 1984, pp 277 – 288 available at: http://www.cs.wisc.edu/~bart/739/papers/end-to-end.pdf

Toumpis, Stavros, 2005. *Topics on Wireless Ad Hoc Networks – Overview*, Telecommunications Research Center Vienna, available at: http://www.eng.ucy.ac.cy/toumpis/courses/ad_hoc/overview.pdf

Toumpis, Stavros, 2005. *Topics on Wireless Ad Hoc Networks – Capacity of Large Networks with Immobile Nodes*, Telecommunications Research Center Vienna, available at: http://www.eng.ucy.ac.cy/toumpis/courses/ad_hoc/mobile_capacity.pdf

# 7 On unabated technological hubris

SAFECOM, *Interoperability Continuum – A tool for improving public safety communications and interoperability*, Department of Homeland Security, available at: http://www.safecomprogram.gov/NR/rdonlyres/65AA8ACF-5DE6-428B-BBD2-7EA4BF44FE3A/0/Continuum080106JR.pdf

ITU-T, Recommendation X.901, 1997. *Information Technology – Open distributed processing – Reference Model: Overview*, International Telecommunication Union, Geneva.

# 8 On combating technological hubris

Borning, Alan, 1987. *Computer System Reliability and Nuclear War*, Communication of the ACM, Volume 30, Number 2, pp 112 – 131, February 1987, available at: http://delivery.acm.org/borning.pdf?

Pearson, David E., 2000. *The World Wide Military Command and Control System - Evolution and Effectiveness*, Air University Press, Maxwell Air Force Base, Alabama, June 2000. http://aupress.maxwell.af.mil/Books/Pearson/Pearson.pdf

Turski, Wladyslaw M., 2000. *Essay on Software Engineering at the Turn of Century*. http://uweb.txstate.edu/~mg43/CS5391/Papers/introduction/essayse.pdf

Worrell, Mike and MacFarlane, Andy, 2004. *Phoenix Fire Department Radio System Safety Project*, Final Report, available at: http://www.phoenix.gov/FIRE/radioreport.pdf

# About Swissphone

Swissphone's goal is to make the most efficient and easy-to-use emergency communication tools. Its dedication to fire and rescue services has led it to develop ways of minimising miscommunication and accelerating quick, joint, responses to emergencies.

## History

Helmut and Erika Köchler established Swissphone in 1969 to design and manufacture pagers.

By the late 1980s, Helmut and Erika Köchler employed about 300 people. Besides tone-only pagers, Swissphone also produces numeric and alpha-numeric pagers.

Swissphone's pagers improved life-saving services provided by doctors, and drastically shortened the response times of the fire and rescue service.

Now, radiopaging is the customary method of leveraging readiness at all levels of public safety.

## A dedicated communication technology

Radiopaging is used primarily to issue warnings to emergency responders, on-site and off-site.

Over the last fifteen years, hand in hand with the transition to fully digital electronic communication technology, paging has developed and spread rapidly. The focus has been on providing greater performance, certainty and ease of use.

Radiopaging is effective in minimising miscommunication, and in avoiding the blockages of vital commands to which other technologies are vulnerable (channel congestion, false calls or denial of service attack).

## Authors

Edouard Dervichian, Director's assistant, Swissphone Telecom AG, tries to assess the impact of policy on the electronic communication sector and on methods of communicating for the safety of the public.

Dorothy Pfister uses lay language to demystify specialised terms and expressions.

* - * - *