© 2004 Elsevier. All rights reserved
Global Economy and Digital Society
E. Bohlin, S. Levin, N. Sung and C-H. Yoon (Editors)

CHAPTER 21

Network Resilience and its Regulatory Inhibitors

James Alleman
College of Engineering and Applied Science, University of Colorado, Boulder

Jonathan Liebenau
Department of Information Systems, London School of Economics, London

Abstract. This chapter explores the rules, regulation, and company actions that impede network resilience. The chapter starts with a definition of network resilience and a discussion of factors that affect it, falling into the three interacting categories of standards, regulation, and government practices and policies. This analysis allows the authors to identify barriers to network resilience related to local exchange carriers (LECs) and electromagnetic spectrum issues, with a focus on rules and regulation that resulted from the Telecommunications Act of 1996. The chapter proposes four main action areas, involving pro-active roles for industry and government actors, for enhancing network resilience: Ensuring inter-modal competition; Stimulating demand for resilience by raising standards; Subsidies to build out critical infrastructure; Devising new governmental roles and priorities. Addressing these concerns, while expensive in parts, will stimulate new business development in the telecommunications industry and is therefore economically justifiable.

1 INTRODUCTION

With the events of 9/11, the concern for network resilience has been foremost on the agenda of the country. The desperate, but often unsuccessful, attempts of people to communicate immediately after the attack on the World Trade Center are the most poignant reminder of the need for communications. While the telecommunications companies responded heroically, and service was restored quickly (Elby 2002, Aduskevicz 2001), many experienced trouble and firms in the Wall Street area and beyond found that the redundancy they thought they had did not exist (United States General Accounting Office 2003a). These firms did not understand that some of the complex rules developed by the Federal Communications Commission (FCC) and mandated by Congress rendered the networks less resilient than they could have been. Many changes are expected in response to the revelations about weaknesses, and also in the normal course of adapting to new conditions of security consciousness and newly available technologies.

However, the current economic weakness of the telecommunications industry is the dominant factor inhibiting investment in network resilience. This weakness has roots in the disillusion of financiers following the "dot.com bubble", the mismanagement of some leading companies, and the detrimental effects of severe competition during a period of high spending for acquisitions, licenses and market share. Many blame the Telecommunications Act of 1996 for some of this weakening; others focus on poor strategic choices and mismanagement in the face of high costs and price-cutting among competitors (Noam 2003). Here we will consider the environment around the telecommunications industry to show what forces are at play and to what extent the network suffers from delay or distortion to the goal of increased resilience.

New opportunities will arise with new thinking about the use of spectrum and the efficient application of new technologies, especially those associated with novel wireless communication devices and architectures. New theories on how to charge for spectrum and how new technologies will allow for spectrum sharing could generate a revised economics of wireless communication that will provide the incentives for investment in resilience.

Effective interoperability and interconnection, a central requirement for resilience, is at least as much a fraught business problem, with policy implications, as it is a technical problem. The current systems of interconnection are also difficult to monitor, to the point where lines are now commonly shared, or conduits are used in common, even where higher levels of independence are expected. How would the disclosure of routing paths affect judgments about reliability and resilience, and what are appropriate rules for interconnection and co-location?

The purpose of this paper is to explore the rules, regulation, and company actions which impede network resilience. We will only be concerned with technical issues insofar as they have impact on the economic and regulatory themes. Initially we address the definition of network resilience and consider the economics and policy areas which affect network resilience. We then explore the ways in which regulation and commercial service and equipment providers create impediments to network resilience. We conclude with an outline of recommendations to enhance the economic/business aspect of network resilience.

2 DEFINITION OF NETWORK RESILIENCE

Before proceeding with the discussion, we need to define what we mean by network resilience. The engineering concept is straightforward: it combines the concept of the "robustness" of a system with the ability to reconstitute itself or to be easily repaired. But what would determine the economic/policy definition of resilience? Resilience must be affordable such that investment and maintenance of a resilient network ensures business viability or at least affordability where subsidies are offered. However, in the long term resilient communications will have to be economical within the normal course of charges for services and any governmental involvement will have to be justified as a reasonable cost to ensure national priorities of infrastructure security.

We combine these ideas by adapting the working notion that network resilience lowers the probability that an event will occur that destroys or disables part of a network such that it cannot be reconstituted – a self-healing network. An example of a resilient network would be a long distance network that, when a major transmission link was cut, was capable of rerouting calls such that the calls were unaffected. Similarly, in a metropolitan network, a SONET ring can provide resilience such that when a cut occurs service can be restored by rerouting around the ring within the accepted 50 millisecond period that allows for transparent voice communication handover. Improvements in network resilience could include incentives to invest in order to make a more robust innovative system or to have more redundancy built into the existing system. It might include the technical ability to make use of alternatives by switching from one form of the network to another (as in transferring calls from the PSTN to the internet through voice over IP). Or, it might be the capability built into systems such that functions can be switched between standard and non-standard usages.

3 FACTORS AFFECTING NETWORK RESILIENCE

Economic and policy factors, in addition to technical ones, have long influenced the engineering character of networks and will increasingly affect their resilience. These fall into three main interacting categories: standards, regulation, and government practices and policies.

3.1 Standards

Standards lie at the heart of network resilience in three ways. Firstly, there is the accepted definition of what constitutes resilience and the tolerance allowable for networks. Currently for voice networks a restoration time of 50 milliseconds is regarded as necessary to ensure transparent handover, and that standard can be met by SONET rings but not by many other standard architectures. The tolerance for handover of data streams can be lower, and a slight lowering of the standard could even now open up a variety of new technologies for consideration as resilient network components. This might especially affect voice over the internet (VoIP) and some of the wireless technologies, including potential networks composed of wireless local area network, IEEE 802.11 standards (especially the widely used WiFi 802.11b technologies).

The other key element of standard concerns the compatibility of hardware and software, and of the use of spectrum, which we address below. Standardization of systems can allow alternative providers of equipment to interface with others when breaks occur and most especially in times of emergency (a necessary but not sufficient condition). The prime example of the lack of compatibility in the United States is the current cellular system. Europe, and much of the rest of the world, adopted the global system mobile communications (GSM) standard, which allows for inter-country roaming and economies of scale in the production of handsets; in principle, the standard also allows for subscribers to utilize the service of alternative providers in time of emergency. New handsets with multiple standards and separate antennae are currently available, but the business model for their use in the United States as well as the regulatory context in which they might operate trail behind the available technology.[6]

For example, the trade-offs between standardization and non-standardization could be examined in the context of using 4-G (and even 3-G) technologies in imaginative ways that provide greater resilience to networks (Techapalokul, Alleman & Chen 2001). There remain many imponderables for future wireless telephony architectures, most especially since the pace of commercial development has slowed following the financial crisis of the telecommunications industry. The extent of consolidation of the industry, and the extent to which

[6] There are those who argue that the development of CDMA technology will be seen in the long run as a positive outcome of the lack of imposed mobile telephone standards in the United States.

competing service providers will be allowed to share networks, will have a major impact on how we might bring forward greater resilience.

One of the concrete proposals to accommodate the financial pressures of the industry insofar as it is overextended in wireless investment is to share certain standard resources. In Europe various types of sharing have been initiated, in some cases, as in Germany, limited to sharing towers (a proposal also popular in other places where property rights and planning permissions make the proliferation of towers problematic, as in Britain) and in others stretching to the sharing of significant elements of the network. Where sharing has occurred it has brought about increased levels of interoperability, sometimes to a limited degree, while in other cases it has been more extensive. Interoperability is usually regarded as a contribution to resilience, but the collocation of facilities, and the multiple usage of apparently redundant elements of infrastructure also have the characteristic of being more vulnerable to attack—one destroyed tower or shared switching facility then doubles the network damage, or worse. In sum, this raises the question, would shared networks, in principle, raise or lower resilience?

3.2 Regulatory Opportunities and Impediments

Legislative and political forces upon the communications industry can enhance network resilience or create roadblocks that inhibit innovations toward more resilient networks. For example, choices about the character of allowable competition have affected the market structure, which, in turn, have an effect on network resilience, as we demonstrate below. Similarly, constraints upon the use of spectrum have an impact on network resilience. A further means would be in adjusting the form of regulation and standards set by bodies such as the Securities and Exchange Commission to guide the way in which financial institutions must ensure that data and communications are adequately protected (United States General Accounting Office 2003b).

Regulators in this industry have usually been mindful of the need to ensure that major investments in commercial technology and in built infrastructure need to be encouraged and to some degree protected. This has meant, in effect, that disruptive technologies have been constrained when they threaten to undermine huge sunk costs early in the investment cycle. Proponents of voice over internet protocol (VoIP) hold this opinion, and many of those enthusiastic about the potential of recent "bottom-up" spreading of wireless local area networks, especially the 802.11b standard (WiFi), believe that the tentative attitude of regulators is delaying what might turn out to be a disruptive technology that could contribute to network resilience. Evidently in Europe the very slow development of WiFi can be attributed to the willingness of regulators to inhibit its use, often on the grounds that it will interfere with spectrum reserved for police and the security services (in Britain and France). It also is seen as a disruptive technology in the context of massive investment in 3G mobile telephony networks (most especially in Britain and Germany).

Regulators do have numerous opportunities to enhance resilience. Currently, for example, the outage reporting system, unchanged for ten years and almost unreformed since its establishment, demands that service providers file memoranda of cuts to service and compile copious data, but fails to use that data in any strategic manner. Outage reports are rarely referred to when issues such as license renewals are discussed, and they are not used to sanction poor performers.[7] Another example of the potential for regulatory involvement could come with requirements to register details of built infrastructure. The absence of accurate maps of switching and conduit systems is a major missed opportunity which regulators, perhaps at the state level, could remedy, especially given the potential for the application of advanced digitalized geographical information systems.

3.3 Government

Although many national security applications such as military communications and the Government Emergency Telecommunication System (GETS) are not directly constrained by commercial financial factors, local governments and civilian applications (including emergency services) are. Government bodies are major consumers of communications services and devices and have the potential to exert more customer pressure on network providers to raise the priority of resilience.

Government users affect prices and demand, and also the opportunities to build out commercial infrastructure to enhance resilience. They also distort the market through their control of large amounts of spectrum. In the years preceding September 2001 much discussion occurred about how new blocks of spectrum could be made available to telecommunications users. It was often noted that the large blocks reserved for broadcasters, especially television broadcasting, were not being used efficiently in the sense that new compression and other technologies are more sparing of spectrum, offering opportunities to relieve some amounts of spectrum. The other large block of spectrum is reserved for military use. Prior to the recent concerns for national security and the needs of the armed forces, there was much discussion of the possibility of releasing some of that spectrum. This proposal is no longer on the table. However, the distorting effects of this kind of governmental control over spectrum has severely limited the availability of non-licensed spectrum, in some cases pressing developers of new technologies to use less efficient spectral bands (such as bands where transmissions are diminished by rain, fog or other atmospheric conditions).

Resilient network improvements must take into account the access prioritization policies of governmental bodies. Currently there are, appropriately, a number of alternative prioritization approaches, ranging from dedicated secure lines to switching priorities in times of network congestion. One of the evident needs of new designs for resilient networks is to ensure that critical services of many kinds, from emergency service workers to national security officers to political leaders, are able to maintain communication when breaks occur in networks. The government is a consumer, a provider, a source of control and an inhibitor of network reliability all at the same time.

In the recent report by the General Accounting Office (2003b), the effects of the physical damage caused by the destruction of the World Trade Center are reviewed and the actions needed to restore services are described. What is perhaps most revealing is the fact that whereas the Security and Exchange Commission has long paid attention to risk reduction efforts, these have not been uniformly applied. In particular, they had not reviewed the broker-dealers' efforts, and it was these members of the financial services community who were most severely hurt and whose continuity of business was seen to be the critical link at the time.

[7] The fact that data are publicly available can be regarded as a service to consumers, and some further analysis is provided by the Alliance for Telecommunications Industry Solutions (ATIS).

Similarly, several federal organization are involved in regulating banks and other depository institutions, including the Treasury, the Federal Reserve and the Office of the Comptroller of the Currency, and all of them have at various times been involved in setting standards or commenting on best practices concerning business continuity and communications.[8]

4 ANALYSIS

In this section we explore the barriers to network resilience, which are the result of government rules, regulation or policy.[9] While these are not deliberate barriers, and indeed, the issues raised by the attacks of September 11th were not considered when the policies were put in place, they nevertheless have significant implications for network resilience.[10] We focus on the 1996 Telecommunications Act (1996 Act), and rules and regulation which resulted from its passage. The 1996 Act was passed single-mindedly to promote competition. However, the impact of the 1996 Act and the resulting FCC rules on network resilience were profound. In this context, we focus on two areas, local (exchange) carriers (LECs) and electromagnetic spectrum issues.

4.1 Local Exchange Carriers

One of the unintended side effects of deregulation following the 1996 Act was that newly introduced players complicated the ability to devise new programs related to resilience. This was largely because such agreements relied on the need to solicit voluntary participation. They also introduced complex coordination of large numbers of key personnel. This affected the way previously existing programs were to work when no longer part of a monopoly. Competition rules are difficult to interpret in practice and most newcomers in the industry are extremely cautious about the appearance of collusion. New players are all competitors, making the sharing of information problematic.

Competition and the consequent larger number of independent players also complicated the ability to react to disaster situations because of coordination problems. Various responses to this have arisen in and around government, including the FCC-linked, industry-organized Network Reliability and Interoperability Council (NRIC) and the Alliance for Telecommunication Industry Solutions (ATIS). We now see a variety of interested bodies, some of which are government influenced (or intended to influence government, both of which can describe NRIC). Others are encouraged or supported by government, and yet others are internal mechanisms. The variety of such bodies has been proliferating and some of them are likely to be better coordinated as the new Department of Homeland Security brings together functions that had been split among bodies such as the FCC, the Department of Commerce and the Department of Defense.

Deregulation falsely raised expectations of users of the ability to have resilience in services by using different carriers when in fact many carriers share the same core network, conduits or

[8] This list could be further expanded to include the Federal Deposit Insurance Corporation, the Office of Thrift Supervision and the National Credit Union Administration.

[9] We will collectively refer to these as policy. The context should indicate whether they are rules, legislation, etc.

[10] We do not pretend that this is an exhaustive list, but merely note what features of policy contribute to reduced resilience.

co-location facilities. This concern was especially raised by customers in the aftermath of the destruction of the World Trade Center when many corporate customers were dismayed to find that whereas they thought they had two independent service providers, what they in fact had were two independent bills for service that passed through some of (or almost all) the same physical infrastructure.

In the United States, the local PSTN is highly concentrated as the result of the historic monopoly of the incumbent local exchange carriers, only four of which are left from the AT&T divestiture in 1984 (Verizon, SBC, BellSouth, and Qwest). In order to promote the development of competition, the Telecommunications Act of 1996 and the FCC's rules implementing the Act required these companies to interconnect with competitors and to unbundle the network and make the unbundled elements available for use by competitors. There are contentious debates about whether such unbundling and interconnection encourages or discourages competition, which we will not deal with here.[11] However, implementation of this "competition" discouraged the deployment of independent, redundant facilities for local communications.

In its attempt to promote competition in the telecommunications exchange market place, the FCC did not distinguish between facilities based or shared facilities competition. It developed three methods through which a (competitor) service provider (so called CLECs) could enter the exchange market – by providing its own facilities, by leasing, at wholesale prices, or by sharing the facilities of incumbent carriers (ILEC). The fastest, easiest, least-risky, and least capital-intensive method of entering the market was by sharing or leasing the facilities of an ILEC. This had several consequences in the development of viable competition in this market. The service was commoditized; that is, there was little to distinguish the various service providers. CLECs were all providing the same service, with no distinguishing features. Thus, they all competed on the basis of marketing.[12]

Financing during the period after the passage of the 1996 Act was easy and abundant. Since competitors did not make investments in facilities, because of the lease/sharing possibilities, they put money into the acquisition of customers. As a result, when terrorists struck, an end-user who thought she had multiple service providers, with multiple paths into the public switched network (PSTN), was distressed to find that all she had was multiple bills, but only one transmission facility – which was no longer operative! Thus, the means by which competition policy was developed had a significant consequence for network resilience. Of course, a monopoly policy might have had much the same effect if this concern were not taken into account, but under monopoly, resilience was a mainstream routine issue, inseparable from other matters of architecture, design and maintenance.

4.2 Electromagnetic Spectrum

Another example in which network resilience is impeded is with electromagnetic spectrum policy. The first issue is the assignment and allocation of spectrum. Both the FCC and other government agencies have responsibility for allocation. Agencies jealously guard the spectrum

[11] This is the topic of work in progress by Alain de Fontenay and Jonathan Liebenau, but one discussion of it can be seen in de Fontenay, Savin & Kiss 2003.

[12] Other issues arose in the drive to develop competition in this market. Bad management contributed to the demise of many of these CLECs; for example, competitors over-estimated the size of their potential markets. (If you added all the projections, many cities show a market more than five times actual size.) But these do not have a direct impact on the subject of this paper.

which they have been allocated, even if they do not use it; the military is the key culprit, but not exclusively. The availability of additional spectrum could enhance network resilience.

The FCC has assumed that proceeds of the spectrum auctions accrue to the government. This has led to inefficient behavior in setting up the auctions. The rationale for auctions is to allocate the resource to its best use. However, because government views the auctions as a revenue source, it attempts to maximize the return from the auctions. This has several effects. The ones we are concerned with are its impact on investment, competitors and resilience.

With respect to investment impacts, the profit maximizing behavior of the FCC reduces the number of potential competitors in this market due to the large, up-front capital requirement which is part of the bid on the spectrum. With fewer competitors, there is less redundancy through duplicate networks. This, coupled with the service suppliers' lock-in behavior (see below), affects resilience. Indeed, in Germany, it is the high cost of 3G spectrum that has driven the winning competitors to petition the regulator for permission to share in the building-out of their networks, with a consequent reduction in redundancy. One can only conjecture about the additional impacts of the high cost of spectrum on the availability of cellular service, the lost R&D etc., which may have indirect impact on resilience.

We must also consider the providers' side, and so we will focus on the wireless industry and its equipment manufacturers. The current cellular markets are robustly competitive, but the competing networks are less interoperable and less interconnected than the PSTN networks. Numerous reasons exist for this lack of interoperability, including purposeful exclusion by the wireless providers in order to "lock in" their customers for business reasons via different protocols, handsets designed exclusively for their systems, and lack of number portability (Shapiro & Varian 1999). As mentioned above, spectrum limitations also inhibited the development of more competitors. However, the prospect of the next generation of wireless offers the possibility of correcting some deficiencies. The statutory and regulatory policies could be changed to improve wireless interoperability and interconnection in order to increase network resilience.

To sketch out the example, in a hypothetical future mobile market we can discern some of the deficiencies of the current system when we consider cellular mobile service. If the regulations/standards for the future cellular mobile system are developed with both competition and resilience in mind, with the various service vendors having to cooperate in questions concerning shared standards for networks and handsets, there would be marked improvements in comparison to today's environment. Thus, if for example the Verizon network were incapacitated, Verizon customers could use Sprint's or others networks that survived. The handset would be designed to work on multiple frequencies and protocols—so called software-defined radio. It could serve as a device that can address WiFi (802.11b) networks, if available. At the next level, if all of the cellular antennas were destroyed, the handset would act as part of an ad hoc network, in effect, each serving as an antenna-relay in order to provide service in the affected area(s). With the handset capable of addressing multiple frequencies, lower bandwidth may be used in self-configuring ad hoc networks because of their promulgation characteristics or other desirable attributes of this spectrum. If the congestion on the network caused the quality of service in the voice network to deteriorate, the wireless IP capability of the handset could still provide communications for the users, either in the traditional mode or the ad hoc network mode.

For emergency personnel (and, perhaps, others), other sensors could be embedded into the handset. The sensors, in addition to locating features, could include gas/bio-warfare detectors that are directly linked to transmission functions. The handsets could contain local building schematics and other attributes of the local buildings—exits, hazard storage areas, etc.— in their memories, serving as enhanced PDAs for emergencies. Of course, with IP capabilities, they could transmit and receive updated information as required (Liebenau 2003).

5 RECOMMENDATIONS

This leads us to a set of recommendations that will be useful in guiding policies both in government and in the private sector over the next few years. Some of these recommendations refer to existing trends, such as the increasing interoperability of handsets, some refer to issues that have long been discussed but which have particular pertinence to resilience concerns, and some are derived from the preceding analysis.

5.1 Categorizing the Problem

Improvements in resilience can be seen to emerge from general changes in the industry; that is, either the continuation of current trends or the application of recommendations broadly agreed upon by observers of the industry. However, there is also a broad category of recommendations that emerge from specific resilience concerns, such as the promotion of particular technologies and direct subsidies (from government or through charges to customers). We address the first only briefly because issues such as spectrum reform and competition policy, while of great importance to resilience, have long been separate areas of debate. While we can show the importance of appropriately resolving these issues, we feel that our major contributions will come from our understanding of new problems and opportunities associated with resilience. The five major problem areas associated with resilience that are in focus in this paper are outlined in Table 1.

Table 1. Resilience Problem Areas

Problem area	Summary description
Congestion	The overloading of pathways, especially in emergencies such that traffic must be rerouted. Denial of service attackers generally use congestion maliciously to overload pathways.
Collaboration and interconnection	The ability to share resources and alter routes and modes. In emergencies and in times of serious congestion mutual aid agreements must be made to work and to accommodate inter-modal communications.
Physical resilience	Protecting facilities from damage; including central stations, conduits, towers, airwaves, etc. Ensure communications and business continuity through distributed facilities and shared capabilities to minimize the effects of physical damage.
Security	Ensuring that routes, messages, procedures, equipment, etc. are safeguarded from intrusion, tampering, distortion, etc.
Emergency response	Immediate patching of damage, rerouting of traffic, and new approaches to communications for emergency workers and those caught up in crises that take into consideration both effective transmission capabilities and appropriate content to inform those involved.

5.2 Solutions

The effort to improve resilience should be undertaken on all fronts and by industry as well as government actors. Below, we describe four solution areas, including specific actions that can be initiated immediately, that should be prioritized:

- Ensure inter-modal competition
- Stimulate demand for resilience by raising standards
- Subsidies to build out critical infrastructure
- Devise new governmental roles and priorities, e.g. support spare capacity

Our first proposal is to maintain inter-modal competition in balance with consolidation. No one system is invulnerable but layers of networks create options, as we currently have in many areas where wireless local area networks, cable modems, personal communication devices, emergency communications systems, mobile telephones, and even powerline communications systems exist alongside plain old wireline telephone systems. This will allow a spread in facilities and avoid the problems associated with, for example, excessive and sometimes uncharted confluence of conduits. We should also encourage moves towards enabling functionality at the network edge (and "dumb pipes") to open networks more and to do this through alliances rather than vertical integration strategies. This is likely to foster solutions such as VoIP and stimulate business and investment, possibly at the cost of traditional wireline service providers. This implies that regulators allow for the imaginative use of spectrum and other delivery mechanisms (we welcome, for example, the recent FCC statements encouraging powerline communications developments) and that competition policies be reassessed to allow for and encourage companies to plan for coordination. We would also wish to see stimulation through experiments sponsored by large users, property developers, local communities, etc. This helps to address elements of all five problem areas associated with resilience.

Second, demand should be stimulated by raising standards for business continuity and communications security. Some mechanisms are straightforward and will attract relatively little objection, such as encouraging best practices for data protection and back-up in critical industries. This could be done with industry cooperation through bodies such as the Securities Industry Association and regulators including the Securities & Exchange Commission, the Treasury and the Federal Banking system. Precedents exist in recommendations for business continuity, and we can learn from the Y2K software improvement campaign. A targeted awareness campaign, bringing together Federal, state and in some places local authorities could educate major commercial customers in all sectors about the value of raising resilience standards. Governmental bodies would also stimulate demand as they improve the resilience of their use of networks, and local authorities should speed up the deployment of E-911 facilities. In the medium term these improvements may not add expenses, especially where high quality solutions reduce risks and maintenance costs. This especially addresses the problem areas of physical resilience and security and encourages spending.

Third, technical solutions need to be investigated and subsidized despite the current inability of companies to invest heavily in traditional research and development. This will require considerable direct funding from government, mainly federal, but also state. Given the current weaknesses at Lucent's Bell Laboratories as well as Telcordia and other commercial sources of telecommunications R&D, competition should be open and available to universities and small independent laboratories, commercial and otherwise. We would prefer to see increases in spending spread widely rather than focused on a small number of special institutions. The National Institute for Standards and Technology might play a bigger role, and large companies should be encouraged to collaborate through neutral bodies, but we would not wish to see the establishment of a national research laboratory. Investments should be made to ensure continued improvements to wireless technologies, especially those like the 802.11xx series of standards. Other areas for special investment might include new approaches to congestion relief, ultra wide band and spectrum switching technologies as well as voice over IP. Considerable further improvements are needed before appropriate customized content can be developed and deployed for emergency uses. This addresses many elements of the five problems areas and will stimulate business development.

Fourth, new roles of governments and some civil society solutions need to be explored, for example as follows.

Federal Jurisdiction

The federal government could make a number of interventions with the potential to improve network resilience. The Department of Homeland Security and other agencies should quickly clarify the role of secure and emergency communications and extend the Government Emergency Communications System (GETS) using wireless, IP and other modes. Federal mandates are needed to ensure spare communications capacity set aside by service providers for emergencies. These would be emanating presumably from the Department of Commerce or the Federal Communications Commission and might be funded by something like the universal services charge. This has long been done with spare capacity requirements for port operators and shippers and for airports and airlines. Federal support is also needed to build up special functions of local law enforcement and emergency services. Here, as in some other areas, there is a need for more transfer of technology from military to civilian uses. Finally, federal grant giving bodies such as the NSF and the Departments of Defense and Commerce should make resilient and emergency communications a top priority.

State Jurisdiction

Public services commissions need to take on more responsibilities for resilience, such as the proposed New York State Public Service Commission's statutory responsibility for protecting infrastructure, which would include specific requirements to maintain vigilance in collaboration with not for profit research, professional and consumer groups and other non-commercial bodies. In addition, state authorities need to ensure that resilience concerns are applied to interconnection rules and offer opportunities to experiment with different approaches.

Local Jurisdictions

At a local level, municipal governments can contribute to resilience in several ways. Resilience associated with local economic development and the defense of local infrastructure and businesses needs to be factored in to municipal functions, as with New York City's Department of Information Technology and Telecommunications. Mutual aid and restoration schemes are also most important in local areas, and municipal governments can encourage compliance by using their market power and through public awareness campaigns.

Civil Society Groups

Voluntary civil action in preparation for emergencies and in times of disaster have been highly effective in solving some problems, such as using advanced communications to notify friends and family, organizing groups to respond where needed, and offering advice to those affected. We could encourage the common use of best practices for solutions such as emergency web portals (E-811), messaging systems, electronic sniffing systems (such as that employed by the Wireless Emergency Response Team—WERT) and other high technology applications. Furthermore, the provision of emergency information content might best be left to civil society groups. For example, voluntary fire departments could coordinate the provision of data suitable for mobile devices to transmit emergency instructions or access special databases relating to property, procedures, risks, etc. Some legal provision might be necessary to ensure compliance and perhaps governmental funding should be provided to meet the cost of data management.

In summary then, we propose to enhance network resilience through the following measures:

1. Encourage inter-modal competition by fostering development and experimentation with new resilient technologies and architectures.
2. Stimulate demand by raising standards for business continuity and communications security.
3. Subsidize new network architecture technologies that promote high capacity and flexibility, especially with regard to wireless and IP technologies.
4. Reassess governmental roles to reflect national security priorities in building out and using communications networks in the manner commonly applied to assure spare capacity in transportation infrastructure.

6 CONCLUSION

We believe that addressing these resilience concerns, while expensive in parts, will all in all contribute to revenues for the communications industry and is therefore economically justifiable. Resilience is functionality worth paying for. Furthermore, funds for homeland security are better spent in the long run in improving communications resilience than, for example, in deploying more armed guards at unlikely targets or inhibiting international trade and travel. The recommendations given will stimulate new business development and provide the means by which service providers can compete based on levels of resilience. They also ensure that innovation and variety are encouraged during this period of economic stringency for the industry.

Each of the capabilities listed above requires engineering, business and regulatory design. For example, software defined radio as described above could currently not be designed and multiple frequencies of electromagnetic spectrum could not be used because of regulatory constraints and rules, even if it is technically possible. Current business practices of the cellular providers contribute to the non-compatibility among handsets. These same business practices do not allow the development of cellular handsets that could take advantage of the unlicensed spectrum used for wireless networks – the 802.11b system (Markoff 2002). Indeed, because of the business conflict among the carriers' own data services planned for the 3G (and beyond), it is highly unlikely that these types of features would be built into the handsets.

The fundamental economic policy question is, who bears the costs of improving network resilience? That question arises not only in relation to our hopes for better architectures or widespread ad-hoc and IP environments, but also with regard to emergency services. We believe that new approaches to enhanced emergency telephony (E-911) should be investigated from a policy and commercial point of view. We have excellent proposals to design emergency content for mobile communication devices, but they raise a flurry of legal, economic and managerial questions that need to be investigated. And there are more imaginative suggestions that are emerging from the interaction of social scientists with communications engineers about the use of the internet during emergencies, as well as other IP-related solutions. These should form the focus of high priority research in the coming years.

7 REFERENCES

Aduskevicz, PJ, "AT&T Response, Terrorist Attack, September 11, 2001" presentation to the Network Reliability and Interoperability Council V, October 30, 2001.

de Fontenay, Savin, Kiss, Submission to the New Zealand Commerce Commission on "Unbundling the Local Loop Network and the Fixed Public Data Network", May 26, 2003.

Elby, S., "Network Design and Resilience", Presentation to Columbia University course ELEN 6901, October 30, 2002.

Liebenau, J., "Wireless Emergency Content" in Valerie Feldmann (ed.), *Wireless Content*, Berlin: 2003.

Markoff, John, "The Corner Internet Network vs. the Cellular Giants," *The New York Times*, March 4, 2002.

Noam, Eli, "How to Cope with the New Volatility", *America's Network*, October 1 2003.

Shapiro, C & Varian, H., "The Art of Standards Wars", *California Management Review*, Winter 1999.

Techapalokul, S., Alleman, J., Chen, Y., "Economics of Standard: A Survey and Framework", Proceedings of the 2nd IEEE Conference on Standardization and Innovation in Information Technology, October 2001.

United States General Accounting Office (a), Report to the Subcommittee on Domestic Monetary Policy, Technology, and Economic Growth, Committee on Financial Services, House of Representatives, Critical Infrastructure Protection, "Efforts of the Financial Services Sector to Address Cyber Threats", Washington D.C., GAO-03-173, January 2003.

United States General Accounting Office (b), "Potential Terrorist Attacks, Additional Actions Needed to Better Prepare Critical Financial Market Participants", Report to the Committee on Financial Services, House of Representatives, GAO-03-414, February 2003.