INTRODUCTION/OVERVIEW

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 of 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-Verizon; AT&T¹; NYT Sept 01], many firms in the Wall Street area and beyond found that the redundancy they thought they had did not exist. 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.

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. Here we will consider the environment around the telecommunications industry to show what

forces 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 new 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 new economics of wireless communication that will provide the incentives for investment in resiliency.

Effective interoperability and interconnection 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 resiliency. We conclude with an outline of recommendations to enhance the economic/business aspect of network resilience.

**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? We adapt 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 not 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.

**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 resiliency. These fall into three main interacting categories: standards, regulation, and government practices and policies.

**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 State is the current cellular system. Europe, and much of the rest of the world, adapted the global system mobile communications (GSM) standard, which allows for inter-country roaming and economies of scale in the production of handsets; and in principle, allows for subscribers to utilize the service of alternative providers in time of emergency (Alleman 2003).² 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.³

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 since the financial crisis of the telecommunications industry. The extent of consolidation of the industry, and the extent to which

³ 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 both accommodate the financial pressures of the industry insofar as it is overextended in wireless investment is to share certain resources. In Europe various types of sharing have been initiated, in some cases, as in Germany, limited to sharing towers (a proposal also popular especially where property rights and planning permissions make the proliferation of towers problematic, as in Britain) 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, 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 low resilience?

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 (Alleman 2002, Liebenau 2002, Liebenau forthcoming, Noll 2002). 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 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.4

4 This is indicated in the recent report of the United States General Accounting Office, Report to the Committee on Financial Services, House of
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 the 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 resiliency. 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 spectrum [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 compiles 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. 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

---

5 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].
about which regulators, perhaps at the state level, could remedy (especially given the potential for the application of advanced digitalized geographical information systems).

**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 (Noam Spectrum, Alleman 19xx). 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 report by the General Accounting Office, 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.

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.6

REGULATORY/POLICY BARRIERS TO NETWORK RESILIENCE

6 This list could be further expanded to include the Federal Deposit Insurance Corporation, the Office of Thrift Supervision and the National Credit Union Administration.
In this section we explore the barriers to network resilience, which are the result of government rules, regulation or policy. While these are not deliberate barriers, and indeed, the issues raised by 9-11 were not considered when the policies were made, they nevertheless have significant implications for network resilience. We focus on the 1996 Telecommunications Act (1996 Act), and rules and regulation which resulted from its passage. The 1996 Act was passed obsessively 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.

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 resiliency. 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. It also 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 into 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

---

7 We will collectively refer to these as policy. The context should indicate whether they are rules, legislation, etc.
8 We do not pretend that this is an exhaustive list, but merely note what features of policy contribute to reduced resiliency.
describe NRIC). Others are encouraged or supported by government, and 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 resiliency in services by using different carriers when in fact many carriers share the same core network, conduits or 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, in fact what they had was two independent bills for service that passed through some (or almost all) the same physical infrastructure.

**Local Exchange Competition**

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. 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 by 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 consequence 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.⁹

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 (Hausman 20xx). 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), found 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, this is not to say that a monopoly policy would improve resiliency.)

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

---

⁹ 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.
Spectrum Auctions

The FCC has assumed that proceeds of the 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 resiliency.\(^\text{10}\)

With respect to investment impacts, the profit maximizing behavior of the FCC reduces the number of potential competitors into this market due to the large, up-front capital requirement required to 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), impacts on resiliency. Indeed, in Germany, it was the high cost of 3G spectrum has driven the winning competitors to petition the regulator for permission to share in the building-out of their networks and the consequent reduction in redundancy.

NOTE ON investment impacts

One can only conjecture the other impacts of the high cost of spectrum on the availability of cellular service, the lost R&D etc, which may have indirect impact on resiliency.

SERVICE AND EQUIPMENT PROVIDERS

As an example on the providers’ side, we will focus on the wireless industry and its equipment providers.

\textit{Wireless}

\footnote{See Alleman 2002 \textit{note} for other issues with the auctions.}
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 [Noam 2001b, Shapiro & Varian 1999]. Spectrum limitations also inhibited the development of more competitors (see above). However, the prospect of the next generation of wireless offers the possibility of correcting some deficiencies [Noam 2001a]. 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 4G market we can discern some of the deficiencies of the current system when we consider cellular mobile service. If the regulations/standards for the 4G cellular mobile system are developed with both competition and resiliency in mind -- the various service vendors can share both their networks and handsets – this would be in marked contrast to today’s environment. Thus, if the Verizon network is 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 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 causes 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 additional to locating features, could include gas/bio-warfare detectors that are directly linked to transmission functions. It could contain in its memory local building schematics and other attributes of the local buildings – exits, hazard storage areas, etc. -- and other features built into them – something like an enhanced PDA for emergencies. Of course, with its IP capability, it could transmit and receive updated information, as required.

**CONCLUSION**

Each of the capabilities listed above requires engineering, business and regulatory design. For example, currently software defined radio as described above could 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 [NYT 04-03-2002]. 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 telephoning (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, and other IP-related solutions. These should form the focus of high priority research in the coming years.