TELECOMMUNICATIONS INFRASTRUCTURE IN DISASTERS:

Preparing Cities for Crisis Communications

Anthony M. Townsend
Mitchell L. Moss

Center for Catastrophe Preparedness and Response
&
Robert F. Wagner Graduate School of Public Service
New York University

http://hurricane.wagner.nyu.edu

April 2005

TELECOMMUNICATIONS INFRASTRUCTURE IN DISASTERS:

Preparing Cities for Crisis Communications

April 2005

Introduction

The breakdown of essential communications is one of the most widely shared characteristics of all disasters. Whether partial or complete, the failure of telecommunications infrastructure leads to preventable loss of life and damage to property, by causing delays and errors in emergency response and disaster relief efforts. Yet despite the increasing reliability and resiliency of modern telecommunications networks to physical damage[1], the risk associated with communications failures remains serious because of growing dependence upon these tools in emergency operations.

The Indian Ocean tsunami of December 2004 highlighted the human cost of communications breakdowns during disasters. While seismic monitoring stations throughout the world detected the massive sub-sea earthquake that triggered the tsunami, a lack of procedures for communicating these warnings to governments and inadequate infrastructure in the regions at risk delayed the transmission of warnings. Yet, based on the successful evacuation of the handful of communities that did receive adequate warning through unofficial channels, it is clear that better communications could have saved tens or hundreds of thousands of lives.

---

[1] W J Mitchell and A M Townsend. 2004. "Cyber agonists: disaster and reconstruction in the digital electronic era", in *The Resilient City: How Modern Cities Recover From Disaster*, L J Vale and T J Campanella, eds. (Oxford University Press: New York)

In the failure to communicate warnings about the impending deluge, news media accounts emphasized the lack of preparation, poor quality of telecommunications infrastructure and geographic isolation of the affected communities as factors.[2] However, as urban disasters over the last decade have shown, even in the most developed economies, catastrophic events routinely overwhelm communications grids. In fact, in these settings the sheer variety and complexity of network infrastructure and the far greater needs and expectations of victims and responders increases the likelihood that any single system may fail. Communications failures in New York City on September 11 contributed directly to the loss of at least 300 firefighters.[3][4] In the 1995 earthquake that struck Kobe, Japan, communications failures prevented outsiders from receiving timely information about the severity of damage. These communications breakdowns delayed relief efforts for days, stranding tens of thousands of homeless victims outdoors in freezing winter weather.

However, modern telecommunications infrastructure has also provided powerful and flexible tools to enable cities to cope with crisis, and quickly relocate and restore displaced or disrupted social and economic activities. The Internet, mobile telephony, and satellite communications provide unprecedented communications capabilities to a wide range of institutions and communities in disaster areas.

This report establishes a framework for understanding the interaction between large urban disasters and telecommunications infrastructure, drawing upon the experiences of the 1990s and 2000s. While the majority of past research on telecommunications in disasters has focused on the emergency response phase, this article analyzes the critical role of communications infrastructure in all of phases of disaster prevention and recovery, which can stretch for years after the event. Finally, this report does not focus only on official communications channels, but is concerned with the entire universe of civil telecommunications infrastructure that plays a crucial role in crisis communications.

This report is organized in the following manner. First, it describes how telecommu-

---

[2] M Kayal and M L Wald. December 28, 2004. "Asia's Deadly Waves: At Warning Center, Alert for the Quake, None for Tsunami." *New York Times*.

[3] National Commission on Terrorist Attacks Upon the United States. 2004. *The 9/11 Commission Report: final Report of the National Commission on Terrorist Attacks Upon the United States (Authorized Edition)*. (W.W Norton & Co.: New York)

[4] McKinsey & Co. 2002. "Increasing FDNY's Preparedness" (City of New York: New York) [http://www.nyc.gov/html/fdny/html/mck_report/index.shtml]

nication infrastructure fails during urban disasters, based on available evidence from several well-documented disasters of the 1990s and 2000s. Then, it examines the role of telecommunications infrastructure, and the consequences of failure, during four key phases of post-disaster recovery: emergency response, restoration and repair, reconstruction, and re-development. It concludes by outlining three areas in which urban telecommunications infrastructure and disaster communications practices can be strengthened to increase their effectiveness in future disasters.

Current domestic preparedness efforts are almost exclusively focused on improving the reliability, capability, and interoperability of official communications systems. However, as we argue in the following section, the full recovery of cities is a multi-stage effort, in which emergency response is only one brief phase. This analysis therefore focuses instead primarily on civil telecommunications infrastructure, which plays a critical role in all phases of disaster recovery - including emergency response.[5]

[5] Evidence from recent disasters clearly indicates that the rapidly advancing capabilities of civilian communications networks, their wider availability, and their widespread standardization have made them indispensable for ad hoc inter-organizational communications among official emergency responders.

How Telecommunications Fails During Disasters

During disasters, telecommunications infrastructure failures occur through a variety of mechanisms. Investigation of communications failures during large urban disasters in the past fifteen years reveals three primary categories of causes:

1. Physical destruction of network components
2. Disruption in supporting network infrastructure
3. Network congestion

This section of the report analyzes each of these three causes of network failure, using historical examples from major urban disasters during the 1990s and 2000s.

Physical Destruction of Network Infrastructure

The most common and well-documented cause of telecommunications failures in recent disasters has been the physical destruction of network infrastructure. Because of the time and funding needed to repair or replace systems, service disruptions caused by physical destruction also tend to be more severe and last longer than those caused by by disconnection or congestion.

As "the most complicated machine ever constructed by human beings,"[6] historically the telephone system has been highly vulnerable to physical destruction during disaster. Earthquakes and severe weather can sever cables and flood underground equipment. During wars, these systems are usually the first sites to be targeted.[7] The destruction of telecommunications networks as a battlefield tactic dates back to the first use of the telegraph in the U.S. Civil War.[8]

The fragility of telecommunications networks is due to the fact that historically, these systems have not had a high degree of redundancy. The telephone network, for example, utilizes a branching structure in which destruction of a single network segment can disconnect entire neighborhoods instantaneously. Cities rarely escape even highly localized disasters without at least some physical damage to the telephone network. The September 11 attacks caused collateral damage to an important telephone routing hub near the World Trade Center, disconnecting large portions of lower Manhattan from the telephone network. High winds in hurricanes and tornadoes, icing in snowstorms, and motion from seismic events all wreak havoc on fragile overhead telephone lines. Underground fires crippled Internet communications on

---

[6] J R Piece and AM Noll. 1990. *Signals: The Science of Telecommunications.* (Scientific American Library: New York). p. 4.

7 See for example E J Felker. 1998. *Airpower, chaos, and infrastructure*. (Air War College, Maxwell Air Force Base, U.S. Air Force) [www.maxwell.af.miłau/auł aupress/Maxwell_Papers/Text/mp14.pdf] and also G R Hust. 1993. *Taking down telecommunications*. Unpublished thesis, School of Advanced Airpower Studies, Maxwell Air Force Base, U.S. Air Force.

[8] "Smithsonian Institution During the Civil War". (The Smithsonian Institution: Washington, DC) [http://www.civilwar.si.edu/smithsonian_siduringthewar.html]

the east coast after the 2001 rail tunnel fire in Baltimore[9], and severely disrupted signaling in the New York City subway system.[10]

Newer telecommunications networks are designed to be more resilient to physical destruction. The development of what would later be called the Internet, starting in the early 1970s, introduced a new philosophy to the design and operation of telecommunications networks. Through both increased redundancy in network connections, and advanced routing techniques to circumvent damaged portions, so-called "packet switched" networks can suffer severe damage before portions of the network become disconnected.[11] The remarkable survivability of IP networks was convincingly demonstrated during one major urban conflict, the 1999 NATO bombing of Belgrade. While major telecommunications facilities were indeed destroyed early on by targeted strikes, Internet service providers were quickly able to fall back to a more decentralized array of secondary links - satellite links, cellular networks, and even amateur packet radio.[12]

Yet despite its potential for resiliency, the Internet is not invulnerable. In fact, as ongoing research has shown, a handful of key interconnection facilities ("telco hotels") located in majors cities present major points of vulnerability for Internet communications.[13] At the local level, Internet service for small businesses and homes is still largely delivered over the old, non-redundant copper wire of the telephone and cable television networks.

Wireless links, whose links are constructed out of intangible electromagnetic radiation, reduce some of the vulnerability of wired networks. Yet as recent disasters have shown, the too are vulnerable to physical destruction.[14] However, wireless networks

---

[9] L Rosencrance. July 19, 2001. "Baltimore train fire disrupts Internet service in Northeast". *Computerworld.*

[10] B Schaller. February 2005. "Learning from the subway fire" *Gotham Gazette*.

[11] P Baran. August 1964. "On Distributed Communications: Introduction to Distributed Communications Network". (RAND: Santa Monica, California)

[12] S Branigan and B Cheswick. 1999. "The effects of war on the Yugoslavian Network". (Bell Labs). [http://research.lumeta.com/ches/map/yu/index.html]

[13] See, for example, the Critical Infrastructure Project at George Mason University. [http://techcenter.gmu.edu/programs/cipp.html]

[14] Wireless links can be disrupted by physical phenomena such as weather or debris.

have a high degree of variability in their vulnerability to physical destruction of nodes, and the loss of service that results. Broadcasting facilities are typically centralized at the metropolitan scale, making them extremely vulnerable. The destruction of One World Trade Center, where many television and radio broadcast antennas were located, disrupted the broadcast capabilities of numerous media outlets.

Newer wireless networks are following the general trend towards more decentralized structures. The cellular telephone network is centralized at a smaller neighborhood scale in major cities. Thus the destruction of antenna sites typically only reduces service in a limited area. For example, McCaw Cellular lost 2 of its 400 cell sites in the Northridge earthquake, resulting in only isolated service disruptions.[15] Emerging wireless technologies such as Wi-Fi serve even smaller areas only a few hundred feet in diameter.

As the most sophisticated and fragile urban infrastructure, telecommunications networks are damaged in nearly every major urban disaster. However, it is not the size of the disaster that is the determining factor, but how its geography of destruction coincides with both old and new facilities for communications.[16]

---

[15] P Andrews. January 21, 1994. "Quake can't shake cellular-phone network". *The Seattle Times*. p. A4.

[16] Remarkably, and counter-intuitively, undersea fiber optic cables in the Indian Ocean survived largely unscathed. One exception was the Malaysian leg of the South-Africa-Far-East (SAFE) undersea cable, where unspecified disruptions caused some traffic to be shunted to redundancy cables and satellite links. N Willing. December 29, 2004. "Tsunami telecom recovery continues". *Light Reading*. [http://www/lightreading.com]

Disruption in Supporting Infrastructure

While less common than outages caused by physical damage, outages caused by disruption in supporting infrastructure tend to be far more widespread and damaging to response and recovery efforts. Telecommunications networks rely upon many other local and regional technical systems to ensure their proper operation. These supporting infrastructures often date from an earlier era and lack resiliency to physical damage.

Electrical distribution systems are by far the most important supporting infrastructure for telecommunications networks. Electrical power is required to operate all modern telecommunications equipment, often in large amounts. Yet electric power distribution systems lack the "self-healing" capabilities of telecommunications networks, although future improvements are expected to give power networks greater capabilities in this area.[17]

In the 1989 Loma Prieta earthquake, 154 of 160 central offices in Northern California lost power. Even worse, back-up power systems at 6 of those 154 failed.[18] During the 2003 blackout in the Northeastern United States, cellular services were severely disrupted because most antenna sites were only provisioned with four to six hours of emergency battery power.

While electrical power systems remain the most important supporting infrastructure for telecommunications facilities, cooling systems are critical and can fail independently of power supply. For example, in the aftermath of Northridge, "interruption of city water service caused some disruption to central office cooling functions."[19]

Finally, failures in transportation disruptions can also impact the supply of fuel for electric power generation. After September 11, a key hub for transatlantic telecommunications - the Telehouse at 25 Broadway - which had already lost its main power supply, was knocked offline due to failures in its backup generators caused by tainted diesel fuel. During the 2003 blackout, the state of Michigan scrambled to locate additional fuel supplies for telephone central office backup generators in an-

---

[17] K E Yeager. 2004. "Electricity for the 21st century: digital electricity for a digital economy" *Technology in Society*. 26:209-221.

[18] A Barnum. January 19, 1994. "Bay Area firms took heed after Loma Prieta". *San Francisco Chronicle.*

[19] EQE International. 1994. "The January 17, 1994 Northridge, California Earthquake". [http://www.lafire.com/famous_fires/940117_NorthridgeEarthquake/quake/00_EQE_contents.htm]

ticipation of an extended loss of power.[20] Finally, the widespread power failures following the 2004 tsunami crippled communications throughout the devastated areas.

Ironically, one of the oldest technologies for telecommunications - amateur radio - remains the only communications infrastructure that has repeatedly demonstrated its ability to operate effectively when electrical power supplies fail. Following major disasters, amateur radio teams working in conjunction with governments and the International Red Cross are rapidly deployed to restore critical basic communications.[21]

[20] Michigan Public Service Commission. November 2003. "Michigan Public Service Commission Report on August 14th Blackout". p. 75.

[21] American Red Cross Amateur Radio Service. [http://www.qsl.net/arcars/]

Disruption Due to Congestion

The final major cause of telecommunications failures during disasters is network congestion or overload. Crises generate intense human need for communication - to coordinate response activities, to convey news and information about affected groups and individuals, and as a panic reaction to crisis. Historically, major disasters are the most intense generators of telecommunications traffic, and the resulting surge of demand can clog even the most well-managed networks. Under this strain, calls are blocked and messages are lost.

The worst case of modern network congestion occurred in the aftermath the 1994 Northridge earthquake. Early morning wire reports in the immediate aftermath stated that "Los Angeles apparently is cut off from rest of world as massive equipment failures and overloaded lines make it nearly impossible to reach area by phone following massive earthquake".[22] Some 204.7 million phone calls were connected nationwide that day by AT&T, making January 17, 1994 the single largest telecommunications event in human history.

Companies such as AT&T dramatically improved their disaster management performance in light of the Northridge experience. By prioritizing the use of circuits for outbound calls, long-distance carriers were able to provide residents of affected areas with the ability to notify loved ones of their whereabouts and status. This information could then be distributed among concerned parties in other parts of the country without creating additional congestion through inbound calls to the affected region. New programs such as the Government Emergency Telecommunications Service "provides emergency access and priority processing in the local and long distance segments" of the telephone network during disasters.[23] These preparations greatly smoothed congestion bottlenecks in the the landline network when the Northridge call volumes were smashed on September 11, 2001.[24,25]

Despite these measures, the pace of development of new and untested communications networks means that failures will continue to occur in new systems upon which

---

[22] A Faiola and T Reed. January 18, 1994. "L.A. communications in chaos". *Miami Herald*. p A11.

[23] Government Emergency Telecommunications Service. [http://gets.ncs.gov/]

[24] V Koptyoff. September 11, 2001. "Communications severely tested". *San Francisco Chronicle*.

[25] P Andrews. January 21, 1994. "Quake can't shake cellular-phone network". *The Seattle Times*. p. A4.

the public depends. September 11, for example, was the first major disaster in which cellular telephone networks were effectively brought down by congestion. According to carriers' reports to the FCC, a ten-fold increase in call volumes during peak hours just after the attacks, led to a 92 percent block rate on New York City's cellular phone networks. In Washington, the blocked call ratio was less severe, but still unacceptable.[26] After the 2004 tsunami struck Phuket, Thailand, cell phone networks (as well as landlines) were congested, leaving only SMS operational.[27]

In addition to the widespread use of untested technologies, congestion failures will remain a common occurrence because of the diversity of inter-linked causes. For example, increasingly complex networks like the Internet often have undiscovered bottlenecks that only become apparent under crisis conditions.[28] In addition, for economic reasons, most communications networks are engineered for peak load at levels well beneath the demands placed on them during disasters. Finally, networks are increasingly subject to attacks based on creating congestion. Such "denial of service" attacks, combined with a a physical strike, are widely suspected to be a future tactic of terrorist organizations.

In the wake of cellular network failures caused by congestion on September 11, the United States federal government moved quickly to establish a priority access system for key public officials. Modeled after the Government Emergency Telecommunications Service (GETS), which provided priority access on the landline telephone network, the Wireless Priority Service (WPS) was designed to manage access to the cellular network in an emergency. However, implementation by carriers has been slow, and participation is voluntary. Although the relevant FCC report and order establishing WPS was issued nearly five years ago, even the urgency of the post-9/11 security environment, only 4 of the 6 major carriers have widely implemented WPS.[29]

---

[26] National Research Council. Computer Science and Telecommunications Board. 2003. *The Internet Under Crisis Conditions: Learning From September 11.* (National Academies Press: Washington, DC)

[27] K Karnjanatawe. February 23, 2005. "Role of ICT in disaster examined". *Bangkok Post*.

[28] National Research Council, Ibid.

[29] FCC Second Report and Order, "The Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Agency Communication Requirements Through the Year 2010: Establishment of Rules and Requirements For Priority Access Service". WT Docket No. 96-86. [http://wps.ncs.gov/documents/242.pdf]

Telecommunications Infrastructure in Disaster Recovery

The first part of this report described three types of telecommunications infrastructure failures during disasters. This section highlights the consequences of these failures by analyzing the role of telecommunications networks in four phases of disaster recovery. This chronology of disaster recovery is based on a system proposed in the 1970s by the NSF-funded research effort on "Reconstruction Following Disaster".[30,31]

This "model of recovery activity" is organized into four phases common across disasters in different regions and historical settings:

1. Emergency responses
2. Restoration and repair
3. Reconstruction of the destroyed for functional replacement
4. Reconstruction for redevelopment

Generally, the duration of successive phases increases by by a factor of ten. While emergency response activities are typically completed with 1-2 weeks, complete reconstruction and redevelopment may take many years.

This framework provides a valuable tool for understanding how communications networks are supplied and used by various participants in response and recovery efforts. The following sections analyze the use of communications infrastructure in each phase: how the phase begins, the role of telecommunications infrastructure in supporting recovery efforts, potential failures of telecommunications networks, and how communications patterns and needs change during transition to the next phase.

---

[30] J Eugene Haas et al., eds. 1977. *Reconstruction Following Disaster.* (Cambridge, Massachusetts: MIT Press)

[31] The authors wish to acknowledge Lawrence Vale of MIT and Thomas Campanella of the University of North Carolina for bringing this research to their attention.

Once a disaster has begun, emergency response activities commence almost immediately through the efforts of bystanders. This period is characterized by "coping actions" stemming from death, destruction, and evacuation. "The emergency period may be very short in societies with a great capacity to cope... lasting only days or a few weeks, or it may drag on for much longer periods of time in societies with a limited coping capacity."[32]

The role of civil telecommunications infrastructure

The most important telecommunications networks during an emergency are official public safety systems. These networks provide skilled emergency responders with the capacity to gather casualty and damage assessment information and coordinate their life-saving and containment activities to the highest degree possible. While prone to failure in extreme circumstances, public safety networks are engineered to provide basic voice communications to support intra-organizational communications during disasters.[33]

Because of the pace of innovation and investment that has occurred since the mid-1990s, increasingly the capabilities of public telecommunications networks match or exceed that of government-administered emergency communications systems. In many cases, such as inter-agency emergency communications, civil networks are the only readily available channels. Particularly in very large disasters that involve official response from multiple government agencies and multiple jurisdictions, the public switched telephone network - both wired and wireless - has become a primary medium for emergency communications. This is because the wide variety of radio equipment used by various public safety organizations is frequently incompatible, preventing communications between responders from neighboring jurisdictions.[34]

Civil networks also often provide greater capability for data communications than their public safety counterparts. Mobile data communications with emergency and law enforcement vehicles, for instance, is often provided over high-frequency bands

---

[32] Haas et. al., Ibid.

[33] For example, 9/11 highlighted several weaknesses in New York City's public safety radio networks, including poor reception in building interiors and underground spaces, as well as capacity constraints. See McKinsey, Ibid.

[34] Several major federal programs are already addressing the critical issue of emergency radio interoperability. It will not be treated here.

with very limited transmission capacity. Alternatively, some jurisdictions that do use public networks have not upgraded their capacity as quickly as networks have evolved. For example, Verizon had to delay decommissioning its obsolete Cellular Digital Packet Data (CDPD) network until 2005 because of an ongoing contract with the Illinois State Police.[35]

Once the disaster event has ended and emergency response can begin in earnest, civil telecommunications networks take on additional critical roles. They convey information in damage assessments, coordinating responses, and relief logistics. Thus, the delivery of communications equipment is often the first priority in providing material relief immediately following a disaster. While public officials direct these efforts, civilians, NGOs and the private sector play a crucial role in providing these capabilities.

Amateur high-frequency and short-wave radio are generally the first communications services to be restored, and the last to be destroyed, in any disaster scenario. Amateur radio is particularly important in isolated, under-developed disaster areas. Following the 20004 tsunami, a handful of "hams"[36] provided the only communications link between the Andaman and Nicobar islands in the Indian Ocean.[37] However, hams play a vital role in developed nations as well. When hurricanes strike in the Caribbean and southeastern United States, hams routinely step in to provide lifeline communications. The Los Angeles County Disaster Communications Service is a group of volunteers who maintain and operate equipment co-located at sheriff's offices throughout the county. "During the first days after the Northridge earthquake, the only link the Granada Hills community Hospital had with the outside world and city government was through amateur radio provided by DCS members."[38]

Non-governmental organizations bear much of the burden of disaster relief, and must make extensive efforts to establish their own communications infrastructures independent of public safety networks - which they rarely have access to. The scope and international nature of the response to the 2004 tsunami highlighted this aspect

---

[35] D Berlind. May 11, 2003. "CDPD is nearing extinction". *ZDNet*.

[36] "Ham" is a colloquial name for an amateur radio operator.

[37] American Radio Relay League. January 7, 2005. "Amateur radio praised as lifeline in South Asia". [http://www.arrl.org/news/stories/2005/01/07/7/]

[38] Los Angeles County Disaster Communications Service. "History of DCS". [http://www.lacdcs.org/history.htm]

of relief deployment. Organizations such as NetHope provide technical solutions and assistance to NGOs, bridging satellite uplinks to local wireless networks to provide turn-key connectivity in even the most remote regions.[39] Corporations like Sony Ericcson also provided provided teams of technicians and 1,300 mobile phones to the International Red Cross effort.

New uses for telecommunications infrastructure often emerge in the heated moments of the emergency response phase. This is particularly true in recent disasters, as rapid innovation in infrastructure has created new, untested communications capabilities. The pressure and urgency of these events has produced ad hoc implementations of new emergency communications schemes. For example, during September 11, personal messaging devices such as the RIM Blackberry were widely used to transmit messages from inside the World Trade Center. An information technology executive at Lehman Brothers, a major investment bank, even activated his company's disaster recovery plan by text message while descending the stairwell of the North Tower.[40] Mobile telephone operators in Sri Lanka were able to issue emergency alerts to foreigners roaming on their networks. Following the tsunami strike, approximately half of these devices were presumed destroyed, providing a basis for estimating possible number of casualties among the tourist population.[41]

The consequences of failure

The emergency phase occurs when the integrity of communications is at the greatest risk. Physical damage is difficult to accurately assess and repair, electrical power is likely to be disrupted, and congestion overwhelms systems optimized for more predictable usage patterns. With lives at risk, it is also the phase where the consequences of failure are the greatest. We can identify three main consequences of telecommunications breakdowns in disaster: paralyzing official responses, challenging containment, and delaying mobilization of broader relief efforts.

In the earliest phases of disaster the focus of official response is on preventing loss of life and, if possible, damage to property. In these urgent moments, any communications failure has the potential to paralyze these efforts, and this scenario has been repeated in disaster after disaster.

---

[39] Dipak Basu, Program Director, NetHope. Telephone interview, January 19, 2005.

[40] *Network World Fusion*. November 26, 2001."Lehman Brothers' Network Survives".

[41] M Williams. 2004. "Asian telecom carriers mobilize after quake, tsunami disaster". *IDG News Service*. December 29.

Congestion is perhaps the most difficult threat to official responders, because its transient nature defies diagnosis. As one analysis argued, "the earthquakes of Kobe, Mexico City (1985), San Francisco (1989), and Los Angeles (1994) [indicate that] telephone networks are not so much destroyed as congested into uselessness."[42] Insufficient capacity in the New York City Fire Department's radio network led to a breakdown of communications at the World Trade Center site during the first attack in 1993.[43] In the 2001 terror attacks, the radio system used by the New York City Emergency Medical Service was severely degraded by congestion caused by panicked operators making unnecessary transmissions.[44]

The second consequence of communications failures during disasters is that they can quickly create an asymmetry in information flowing into and out of the affected area. In practice, across a wide range of public and official networks, it is far easier to communicate out from a disaster area than to initiate communications to someone located within. (Note before, this is AT&T explicit policy!) In combination with the fact that many people within the disaster area will be cut off from basic telecommunications, outside observers frequently have more information about events unfolding in the affected area, the extent of damage, and the location and nature of the response. The rumors resulting from such information gaps - false warnings of aftershocks, epidemics, counterattacks - can cause widespread panic and irrational behavior that undermines response and relief efforts.[45]

Finally, breakdowns in emergency communications can significantly delay mobilization of broader relief efforts that involve non-official responses to emergencies. The 2004 tsunami illustrates an extreme case because it occurred in a region in which there was virtually no emergency communications capability available after the event. What little pre-existing communications infrastructure survived in the most heavily damaged areas was compromised by power failures. Even the first wave of

---

[42] E M Noam and H Sato. 1996. "Kobe's lesson: dial 711 for "open" emergency communications" *Science*.

[43] "Report from the Chief of Department, Anthony L. Fusco," in William Manning, ed., *The World Trade Center Bombing: Report and Analysis* (FEMA, undated), p. 11.

[44] M Moss and A M Townsend. 2003. "Response, restoration, and recovery: September 11 and New York City's Digital Networks" in *Crisis Communications: Lessons from September 11*. A Michael Moll, ed. (Rowan and Littlefield)

[45] E L Quarantelli. 1989. "The social science study of disasters and mass communication", in *Bad Tidings: Communication and Catastrophe,* L M Walters et al, eds. (Lawrence Erlbaum Associates: Hillsdale, New Jersey)

international responders faced delays in getting emergency communications established. It was not until December 31, 2004 that five Red Cross Emergency Response Units (ERUs) specializing in telecom, water and health care were on the ground in Sri Lanka.[46] More than a week after the disaster, senior UN relief coordinators admitted that communications were still lacking.[47] As of January 4, 2004, Oxfam's NGO Coalition operations center in Bakongan was still without communications.[48]

Transistioning to restoration and repair

The emergency response phase ends with the termination of search-and-rescue operations and the clearance of debris from major streets. As a civil defense manual on restoring transportation stated in 1954, communications plays a critical role:

> Advance planning should prepare the restoration group to function with minimum supervision from the main control center. This is especially important when there is the possibility of a breakdown in communications... Each operating base should have telephone and two-way radio communications with the chief of the roads and bridges branch at the main control center... The chief of engineering services should work with local telephone companies to insure that in time of emergency these companies can provide essential communications. In a major disaster, many telephone communications facilities would probably be destroyed; therefore, radio communications should also be made available.[49]

While the critical work of debris clearance and restoration of streets for basic access can be conducted using messengers and face to face instruction, telecommunications allows greater control, more accurate status reporting, and better integration with other efforts.

---

[46] International Federation of Red Cross and Red Crescent Societies. Dec 31, 2004. "Red Cross volunteers' relief effort for tsunami victims in full swing".

[47] *Turkish News (via AFP)*, January 6, 2005. "Annan says a billion dollars needed as UN takes over relief operation".

[48] Oxfam GB, Ltd. January 4, 2005. "Oxfam Has Sent Kiwi Engineers to Aceh".

[49] Federal Civil Defense Administration. 1954. *Clearance and Restoration of Streets and Highways in Civil Defense Emergencies*. (U.S. Government Printing Office: Washington, DC). p.8, 11.

For telecommunications infrastructure itself, the transition to the next phase, restoration, generally occurs quite quickly. The temporary loss of performance caused by congestion generally subsides as order is restored, and demands for communications are reduced. Telecommunications providers also have become highly agile in responding to physical destruction. After a major switching facility was destroyed in the World Trade Center on September 11, AT&T's response was so rapid that many of its vehicles were detained at entry points to Manhattan - the firm was ready but public officials were not. Finally, many newer telecommunications networks are designed to be "self-healing", and can begin restoring themselves almost immediately after links are broken.[50]

[50] R Poor et al. 2003. "Wireless networks that fix their own broken communication links may speed up their widespread acceptance". *ACM Queue*. 1(3).

Telecommunications During Restoration and Repair

The second phase of disaster recovery "is characterized by the patching up of the utility, commercial and industrial structures" that can be repaired, and the resumption of normal social and economic activities.[51] This restoration phase begins when search and rescue operations have been concluded, and basic transportation and communications capabilities have been re-established.

In recent disasters, especially in developed nations that have high rates of personal ownership of computers and mobile phones, telecommunications has been a powerful tool in helping rapidly resume normal social and economic activities.

While "tele-working" or "telecommuting" received considerable attention from pundits and futurists in the 1980s as a means of reducing congestion and commute times, it was the two California earthquakes (1989, 1994) that that first provided the impetus for large-scale implementation. Because of extensive damage to regional freeway networks, many firms quickly established telecommuting centers that helped workers return to work while many more worked from home using personal computers and modems.[52] While widely believed to be a temporary measure, approximately eight months after the Northridge earthquake reports indicated that 9 out of 10 post-disaster telecommuters Los Angeles area were continuing to do so.[53] Telecommuting by displaced workers from Lower Manhattan, such as the 334 employees of the Securities and Exchange Commission in Lower Manhattan, were also largely temporary.[54] However, many private firms began to rely on telecommuting after September 11 and this practice has continued long after the event.

Mobile phones have become increasingly important in post-disaster resumption of normal life. Used in peacetime to organize complex daily activity patterns across sprawling cities, mobile phones provided a flexibility and feeling of security and connectedness vital to survival in unpredictable post-disaster urban landscapes. "After the 1989 Loma Prieta earthquake, Cellular One experienced an immediate 20 percent jump in minutes of air time used in the greater Bay Area. The higher usage never de-

---

[51] Haas, Ibid.

[52] J Eckhouse. January 20, 1994. "L.A. Firms Look to High Tech For Way to Beat Traffic Mess". *San Francisco Chronicle*. January 20.

[53] *Los Angeles Daily News*. September 10, 1994. "Quake shakes worker habits".

[54] J Dean. December 1, 2001. "Disaster and recovery". *GovExec.com.*

creased, apparently because so many people purchased cellular phones to bolster communications after the quake. McCaw Cellular Communications said sales of cellular phones in its Bay Area territory jumped 43 percent over projected growth in November 1989, the month after the Loma Prieta quake."[55]

Mobile Phone Penetration During Major U.S. Disasters, 1989-2004[56]

Date	*Event*	*Mobile Phone Lines*	*Mobile Phone Lines Per 100 Persons*
1989	Loma Prieta earthquake	3,508,944	1.4
1995	Northridge earthquake	33,785,661	12.9
1999	Hurricane Floyd	86,047,003	31.6
2001	September 11 attacks	128,374,512	45.1
2003	Northeast blackout	158,721,981	54.6

The Internet and World Wide Web are another set of technologies that have transformed the way key restoration and repair functions are conducted. The Internet's value in disaster was first seen in the immediate aftermath of Northridge and Kobe, where it provided an alternative means of communications and news.[57]

A decade later, the Internet had evolved into a global mass medium reaching some 1 billion people, and its role in disasters had increased correspondingly. Less than three weeks after the 2004 tsunami, a variety of charitable organizations collected an estimated $500 million in relief donations through the Internet.[58] Cleared in under 72

---

[55] Eckhouse, Ibid.

[56] Author's calculations based on Cellular Telephone Industry Association. "Semi-Annual Wireless Industry Survey". [http://www.ctia.org/research_statistics/statistics/index.cfm/AID/10030] and National Population Estimate Series, Population Division, U.S. Census Bureau.

[57] R G McLeod. January 18, 1995. "Even the Internet was Shaken Up". *San Francisco Chronicle.*

[58] "Fundraising for Tsunami Relief Transformed by Internet". January 11, 2005. *PND News*. [http://fdncenter.org/pnd/news/story.jhtml?id=92200034]

hours, these funds could be applied to relief efforts much faster than before, when organizations had to wait to receive funds by mail.[59]

Finally, during the restoration and repair phase, telecommunications networks themselves must be patched to support ongoing relief efforts and eventual recovery. While it is more likely to be damaged, compared to other urban infrastructure, the restoration of telecommunications networks is generally more rapid (though not necessarily less costly). Following the September 11 attack, the local telephone company was able to restore service to the New York Stock Exchange in just a few days by transferring equipment from other locations to replace some three million disconnected lines. Even in developing countries, telecommunications is one of the first services that can be restored to service. Just four days after the 2004 tsunami, two-thirds of the telephone exchanges on Car Nicobar were operational. In Sri Lanka, just 10,000 of the country's 1.8 million telephone lines were out of service due to damage from flooding in Hambantota.[60]

The use of wireless technologies to rapidly restore communications services has become increasingly widespread. Following September 11, a wide range of point-to-point wireless patches were deployed to reconnect Manhattan's Financial District to New Jersey and Brooklyn, including free-space optics (laser) and microwave technologies. These links were established rapidly, within a matter of days, and have since been widely adopted as a permanent backup.[61] Local business groups in New York have pursued an ambitious plan to create a rooftop mesh of wireless links that would let neighboring building provide redundant communications to each other.[62] Rapidly deployable temporary cellular sites, an innovation that grew out of the Northridge experience, have been widely used to restore mobile phone service in nearly every major disaster since. Finally, the rapid deployment of Wi-Fi and other unlicensed broadband wireless technologies at disaster sites provides an easy way to bring broadband to critical relief facilities without extensive cable deployments.

---

[59] A Gonsalves. January 4, 2005. "Tsunami Relief Efforts Get Record Online Donations". *Internet Week*

[60] N Willing. December 2004. *Light Reading.* [http://www.lightreading.com]

[61] J Wexler. February 14, 2005. "Why WiMax". *Computerworld*. p.26.

[62] J Silbert. June 2003. "NYC, Inc.: Call for Backup: The wireless way to make downtown's telecom system more secure than ever before". *City Limits*.

Transitioning to reconstruction

The return of refugees, complete clearance of debris, and the functioning of major urban services and utilities such as transportation mark the end of the restoration phase. This phase is generally concluded within several months. For example, the massive operation to clear debris from the World Trade Center collapse was completed in approximately 9 months, well ahead of the schedule initially anticipated.

Telecommunications During Reconstruction

The reconstruction phase is characterized by a return of population, capital stocks and economic activity to its pre-disaster levels or greater, which generally occurs within a few years. The replacement of telecommunications infrastructure is a high priority during this phase, and contributes significantly to supporting other reconstruction efforts.

The reconstruction of landline telecommunications networks can a time-consuming and expensive process. For example, the telephone company Verizon projected the cost of rebuilding its infrastructure in and around its 140 West Street hub at between $1.1 and 1.4 billion.[63] However, in recent disasters, wireless technology is providing more rapid and flexible options for reconstructing telecommunications networks.

The post-war reconstruction of Iraq's devastated telecommunications infrastructure highlights the way in which wireless technologies are being used to shorten the time needed for replacement, as well as to provide flexible tools supporting a return to pre-disaster levels of social and economic activity. One of the first major set of reconstruction contracts issued by the occupation authorities were for mobile cellular telephone services. "The speed with which mobile networks can be established compared to landlines makes these wireless contracts far more valuable in developing states and post-conflict situations."[64] Similarly, in Kosovo, following the ethnic conflict and NATO intervention, a GSM mobile cellular network was deployed in the capital city of Pristina to "provide essential communications pending full reinstatement of the fixed network."[65]

Not all wireless technologies are equally versatile, however. Ironically, depsite its simplicity and long track record, traditional broadcast infrastructure has shown itself to be more challenging to reconstruct. Following the collapse of the north tower of the World Trade Center, some 1500 rooftop antennas were destroyed - many of which served the region's television and radio broadcasters. The roof of the towers was an ideal broadcast platform, with clear line of sight 100 miles in every direction. Of the seven primary broadcast television networks serving the New York metropoli-

---

[63] B Woller. March 2, 2002. "Utilities continue push for funding to rebuild lower Manhattan" *The Journal News*.

[64] Open Society Institute. 2003. "Iraq's Reconstruction Contracts: Telecommunications". Revenue Watch project, Report No. 2, p 2.

[65] European Commission. April 2000. *Kosovo: Reconstruction 2000*.

tan area, only one network (WNYW-5) whose primary broadcast facility was on the Empire State Building, was unaffected. As the table below shows, the other networks employed a variety of strategies to restore partial service. For many broadcasters, however, it will require the full reconstruction of the World Trade Center's replacement to achieve equal broadcast capability.

Status of Broadcast Television Stations in the New York Area After September 11

Channel	Network	Status as of October 2001
2	WCBS	Broadcasting from a lower-power backup facility on the Empire State Building.
4	WNBC	Broadcasting from a lower-power backup facility located in Alpine, NJ.
5	WNYW	Not affected - primary site on Empire State Building.
7	WABC	Broadcasting from a lower-power backup facility located in Westchester County, NY.
9	WWOR	
11	WPIX	Re-broadcasting on UHF channel 64.
13	WNET	Broadcasting from a lower-power backup facility located in Alpine, NJ.

Transitioning to redevelopment

The shift from reconstruction to redevelopment in recent disasters is a difficult distinction, because the rapidly advancing state-of-the-art in communications technology often means that replacement is often an improvement. Reconstruction of pre-disaster telecommunications networks with today's equipment often means upgrading its capabilities significantly.

However, these experiences also teach us that the broader transition from recon-

struction to redevelopment also brings a fundamental rethinking in the way telecommunications networks are constructed and managed, and the way they contribute to betterment of the city.

Telecommunications During Redevelopment

The final phase of recovery from disaster proposed by Haas is "the commemorative, betterment, and developmental reconstruction period", which we call *redevelopment*. In contract to reconstruction, redevelopment is a longer process that may stretch over decades, but entails significant large, often government-funded projects that serve future growth and development. Often these investments seek to prevent or mitigate future disasters, and launch the city onto a new post-disaster trajectory of prosperity and security.

Public warning systems, whose failure so clearly leads to loss of life, typically receive the bulk of attention and effort to improve communications after a disaster. In the wake of the warning failures of the 2004 tsunami, the United Nations has launched a International Early Warning Program aimed at "the reduction of the growing impacts of disasters, through the development of more systematic approaches to the use of early warning of the conditions that lead to disasters".[66] The failure to activate the United States' primary public warning system on September 11, the Emergency Alert System, has been widely criticized.[67] The outcome of these public warning failures is significant investment throughout the world in public warning systems.

Disasters also focus attention on the need to manage network congestion during emergencies, and to provide priority access to public officials and key civilian responders. The recognition of the importance of the public cellular telephone network in coordinating complex multi-agency responses to large disasters has spurred the deployment of priority access to that service through the Wireless Priority System. In place during the 2003 blackout, this system performed as expected. Priority users experienced a 95 percent success rate making calls using the prioritized system.[68] Voice over Internet Protocol (VoIP) is also being touted as a way to "engineer... survivability during disaster scenarios that involve the failure of network components and/or extremely high call volumes that often occur during times of regional or national crisis."[69] Many organizations affected by September 11 accelerated

---

[66] United Nations International Strategy for Disaster Reduction. Platform for the Promotion of Early Warning. [http://www.unisdr.org/ppew/]

[67] L K Moore. 2004. "Emergency Communications: The Emergency Alert System and All-Hazard Warnings". (Congressional Research Service: Washington, DC)

[68] W Jackson. August 18, 2003. "Emergency telecoms program gave responders access". *Government Computer News.*

[69] "Voice disaster recovery". Internet2 VoIP Working Group. [http://voip.internet2.edu/dr/]

planned VoIP deployments after the communications disruptions that followed the attacks.[70]

At the physical level, redevelopment of telecommunications following recent disasters has emphasized structural redundancy as a "crucial" and "indispensable" means to cope with the threat of physical destruction.[71] The new regional disaster management network in Kobe, Japan uses multiple redundancy to prevent a recurrence of the physical destruction that isolated the region during the 1995 earthquake.[72] In New York City, several efforts illustrate this approach to improving telecommunications networks. The municipal government has recommended the development of carrier-neutral ducts that would provide additional route diversity.[73] A group of property owners and local businesses in Lower Manhattan has proposed the deployment of a cooperative mesh of rooftop wireless transmitters that would create a redundant net of connectivity to adjacent buildings.[74]

Technological advances are also presenting the opportunity for major improvements in mobile data communications for emergency responders. American cities are leading the way, investing an estimated $50 to 100 billion in emergency response preparedness over the 2004-2009 period. At least $17.2 billion has been budgeted for deployment of interoperable emergency communications networks and implementation of E911.[75] New York City alone plans to spend $1 billion on a citywide mobile public safety network, utilizing channels in the 4.9 Ghz range reserved for public

---

[70] S Breidenbach. 2002. "Terrorist attack kicked VoIP pilot program into high gear." *Network World Fusion*. August 12. [http://www.nwfusion.com/techinsider/2002/0812convergemcc.html]

[71] President's National Security Telecommunications Advisory Committee. April 2004. *Financial Services Task Force Report.*

[72] Disaster Management Bureau. "Network of the Phoenix Disaster Management System". (Hyogo Prefecture, Japan). [http://web.pref.hyogo.jp/syoubou/english/phoenix/ph4.html]

[73] City of New York, Department of Information Technology and Telecommunications. December 2002. "Request for Proposals for Franchises Authorizing Construction and Provision of Lateral Ducts and Related Facilities to House Telecommunications Fiber Links Transmitting Local High-Capacity Telecommunications Services Between Mainline Systems and Building Entrances." [http://www.nyc.gov/html/doitt/downloads/pdf/lateral_ducts_rfp_122002.pdf]

[74] Alliance for Downtown New York, Association for a Better NY, the Real Estate Board of NY and NY Building Congress. August 2002. B*uilding a 21st Century Telecom Infrastructure: Lower Manhattan Telecommunications Users' Working Group Findings and Recommendations*. [http://www.downtownny.com/assets/TelecomReport.pdf]

[75] R A Clarke, J F Metzl and W B Rudman. June 2003. "Emergency Responders: Drastically Underfunded, Dangerously Unprepared" (Council on Foreign Relations: New York, NY)

safety. This system will provide four sets of services: high speed data and video, automatic vehicle location, call boxes, and traffic signal control.[76]

Industry, while in many ways better prepared to handle disaster than the public sector, has used recent disasters to restructure its business practices to ensure greater "business continuity". Important standards-setting organizations such as the National Fire Protection Association, in conjunction with the Federal Emergency Management Agency, have promulgated information about how business should prepare for disaster management and business continuity.[77] Particular attention has been focused on maintaining the integrity of critical financial and economic infrastructure. As a Presidential advisory board stated, "...neither the Federal government nor a critical infrastructure can respond to a national-level crisis without critical infrastructure sectors employing strong business continuity and disaster responses planning practices."[78]

Finally, the least tangible, but potentially most significant lasting reconstruction "project" is the re-location of economic activity in response to real or perceived threats in the post-disaster period. While tele-commuting by individuals in the days and weeks after disasters now appears to be a fairly common response to disruptions in transportation systems, there has not been systematic study of how long these practices continue. Urban planners have pointed to New York's experience following September 11 to argue that disasters (at least ones caused by terrorism) do not appear to be linked to wider economic decentralization over the long-run.[79] As evidence, they cite reports that three-quarters of the firms (and jobs) displaced by the attacks returned to or remained in Manhattan.[80][81] In terms of jobs, the picture is slightly less rosy, However, given New York's unique role as a global financial hub, cultural center,

---

[76] Department of Information Technology and Telecommunications. March 24, 2004. "Request for Proposals: Citywide Mobile Wireless Network". (City of New York)

[77] National Fire Protection Association. *NPFA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs: 2004 Edition.* (NPFA: Quincy, Massachusetts)

[78] President's National Security Telecommunications Advisory Committee, Ibid. p. 20.

[79] P Eisinger. 2004. "The American city in the age of terror: A preliminary assessment of the effects of September 11". *Urban Affairs Review*. 40(1):115-130.

[80] New York City Partnership. 2002. "Vital signs: Economic realities and challenges facing New York City one year after 9/11". (New York, New York)

[81] [M L Dolfman and S F Wasser. June 2004. "9/11 and the New york City economy: A Borough-by-borough analysis". *Monthly Labor Review* (Bureau of Labor Statistics)

and immigrant entrepôt, and the local and national emotional significance of the attacks seems to make it a poor case from which to generalize.

Preparing Urban Infrastructure for Crisis Communications: An Agenda for Research

This report has analyzed the importance of telecommunications infrastructure in understanding how cities respond to emergencies and recover from disaster. The rapid pace of development of these systems has provided valuable new capabilities to both official and unofficial responders and providers of relief. Yet at the same time, failures in critical telecommunications systems are becoming an all-too-common common fixture in unfolding disasters. These failures led to preventable loss of life and damage to property, hindering relief efforts, and undermine the long-term recovery and redevelopment of our urban centers.

In the United States, an estimated $50 to 100 billion was being spent on emergency response preparedness. The amount devoted to communications is unclear, but one commission noted that as much as $20 billion in additional spending on interoperability and E911 projects communications needs is projected.[82] However, federal investments to date suffer from several important shortcomings:

1. They only address the emergency communications needs of official responders only - ignoring the broad set of key private sector and NGO responders.

2. They focus only on the emergency response phase, and ignore communications needs during the rest of the long recovery process.

3. They rely too heavily on new technologies that are untested in disasters, while ignoring new technologies and practices that emerge from the ground-up during disasters.

4. They do not adequately anticipate extremely large, high-consequence disasters.

Granted, federal efforts to date have been focused on providing remedies to the most immediate emergency communications challenges facing official responders after 9/11 - interoperability, public warning systems, and 911. However, with these programs underway, the time is right to address these broader shortcomings through research and policy action. The federal government needs to being exploring what kinds of tools, guidance and assistance it can provide to prepare the private sector and non-

[82] R A Clarke, J F Metzl and W B Rudman. June 2003. "Emergency Responders: Drastically Underfunded, Dangerously Unprepared" (Council on Foreign Relations: New York, NY)

government organizations that actually provide the bulk of response and recovery efforts. As Gordon Gow succinctly puts it, "in short, the history of emergency telecommunications has been reactive rather than proactive."[83] The goal of this report is to outline a framework for a far-reaching research agenda in crisis communications preparedness for American cities.

This report recommends increased research in the following six policy and technology areas of emergency and disaster communications:

1. Preparing the Private Sector and NGOs for Disaster Communications
2. Improving the Reliability of Public Networks
3. Leveraging New Communication Technologies and Practices
4. Risk Management, Telecommunications and Urban Decentralization
5. Rethinking Public Warning Systems
6. Modernizing the Amateur Radio Service

[83] G A Gow. 2005. "Emergency telecommunications and mitigation-oriented policymaking". *World Dialogue on Regulation.* [http://www.regulateonline.org/content/view/254/32/]

1. Preparing Private Sector and NGOs for Disaster Communications

Three decades of social science research in disaster recovery has produced a compelling body of evidence on the important response role of private firms, NGOs, and social networks.[84] International aid agencies are increasingly orienting disaster preparedness and prevention strategies around these institutions.[85] Particularly in very large or prolonged disasters that exhaust official capabilities, NGOs and citizen volunteers are crucial.

Growing adoption of business continuity planning, a set of practices aimed at ensuring that essential functions can continue after a disaster, is providing a model for action. However, very little is known about the extent of business continuity plan adoption in the private sector (aside from the financial services sector), nor how emerging standards such as NFPA 1600 apply to NGOs.[86]

There is also little understanding of how to meet the communications needs of international disaster relief operations more effectively. Technological limits, funding issues, and regulatory differences all create obstacles to rapid deployment of communications services to support relief and recovery efforts. While some progress has been made in easing import and licensing restrictions on donated telecommunications equipment in disaster zones, many research questions remain.[87]

Key future research needs include:

- What are the barriers to business continuity planning in private firms and NGOs?
- What do business continuity standards like NPFA mean for NGOs, and are they being implemented? How will this affect their ability to perform their missions?
- How can we assess the adoption of business continuity standards, and their effectiveness at preserving a response effectiveness in key private sector and NGOs?

---

[84] E L Quarantelli. 1997. "The Disaster Research Center (DRC) Field Studies of Organized Behavior in the Crisis Time Period of Disasters". (Disaster Research Center, University of Delaware)

[85] United Nations Center for Regional Development. January 17, 2003. "From Disaster to Community Development: The Kobe Experience". [http://www.hyogo.uncrd.or.jp/publication/documents/kizuna.pdf]

[86] National Fire Protection Association. 2004. *NFPA 1600: Standard on Disaster/Emergency Preparedness and Business Contiunity Programs: 2004 Edition.* [http://www.nfpa.org/PDF/nfpa1600.pdf]

[87] "Disaster zones to get easier telecoms deployment". January 11, 2005. *Cellular News*.

2. *Improving the Reliability of Public Networks*

A key lesson of September 11 is that our increasingly complex infrastructure for telecommunications is no longer under the control of a single entity that can be held to standards of reliability. The regulated regional telephone companies that used to pride themselves on the reliability of their service, have been replaced by competitors and competing technologies. The three major broadcast networks are now supplemented by hundreds of cable and satellite networks. Vertical disintegration, particularly in the provision of Internet services, has led to layered infrastructure that further complicates the goal of network reliability. Finally, our increasing dependence upon the limited capacity and fickle nature of wireless networks remains the great unspoken Achilles' heel of emergency telecommunications.

Despite the failures of civil telecommunications networks in recent disasters (summarized in tabular form in Appendix I), only scattered efforts have been undertaken to improve their overall reliability. And in fact, many disaster scenarios implicitly assume "that most of the country will have largely normal communications... and that affected areas will have some level of communications."[88] As in the case of New York City's voluntary Mutual Aid and Restoration Compact, which "sets up procedures for competing telecommunications carriers to cooperate after a major telecommunications outage", these efforts are confined to the few regions highly dependent on financial services.[89],[90] It is increasingly clear that effective solutions will require regulatory, economic, and political adjustment in addition to purely technical ones.

In Lower Manhattan, several financial institutions discovered on September 11 that despite their best precautions to secure diverse telecommunications connections to their facilities, many of these networks were actually routed back to same local

---

[88] W H Ware. Date unknown. "The cyber-posture of the national information infrastructure". (RAND: Santa Monica, California)

[89] New York City Economic Development Corporation and Department of Information Technology and Telecommunications. 2005. *Telecommunications and Economic Development in New York City: A Plan for Action.* (City of New York)

[90] San Francisco Telecommunications Commission. 2004. "Update to the Telecommunications Plan". (City of San Francisco, California)

switching facilities.[91] Despite pressure from state public service commissions, incumbent carriers have successfully resisted efforts at public oversight of network reliability.[92] A Presidential Advisory Committee charged with studying the financial industry's telecommunications preparedness offered little more than an endorsement of the current meager efforts and found no role for government in developing, enforcing, or monitoring standards.[93] Finally, recent administrative decisions on network reliability are working to undermine the public's ability to monitor the state of infrastructure operations. For example, in August 2004, citing security concerns, the FCC has stopped providing the public access to network outage data.[94]

Research questions:

- How can we assess the current state of reliability of complex, fragmented and hidden telecommunications infrastructure?[95]
- How can network reliability be prioritized in local planning and telecommunications regulatory activities?
- How does the reliability of new networks like the Internet and cellular telephone systems compare to existing systems? While expert panels have found that the Internet proved remarkably resilient to collateral damage in recent disasters, it remains extremely vulnerable to targeted attack.[96]
- What are best practices in regulation and implementation at the national, state, and local level to ensure network reliability?

---

[91] Lower Manhattan Telecommunications Users Working Group, Ibid.

[92] New York State Public Service Commission.

[93] President's National Security Telecommunications Advisory Committee, Ibid.

[94] C Stern. August 28, 2004. "FCC cuts public line to phone outage data". *Washington Post.* [http://www.washingtonpost.com/wp-dyn/articles/A40329-2004Aug27.html]

[95] T H Grubesic and A T Murray. 2005. "Geographies of imperfection in telecommunication analysis". *Telecommunications Policy*. 29(2005)69-94.

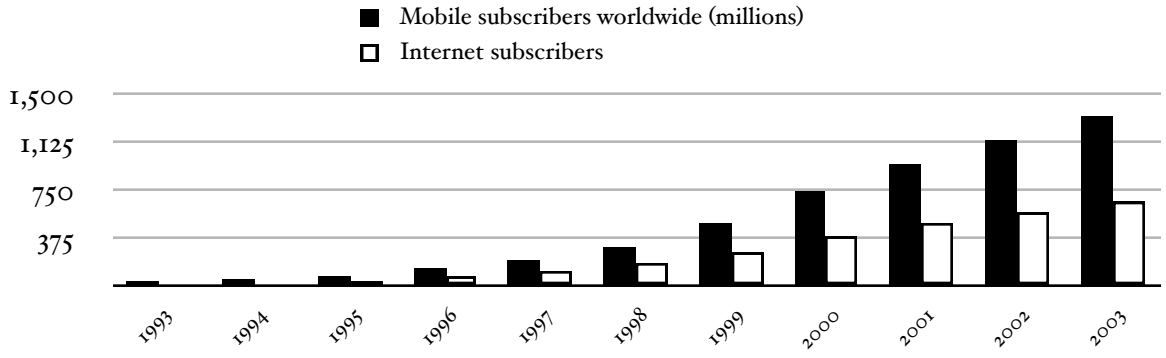
[96] National Research Council, Ibid.

Some of the greatest success stories from recent disasters have come from the ways in which new technologies have been applied in unanticipated ways to solve timeless challenges of emergency communications. These new practices need to be systematically examined, and where appropriate, integrated into preparedness efforts. Efforts to encourage creative approaches to emergency communications must be encouraged.

One model for how this might be done can be found in the Internet Society's recent Public Warning Challenge.[97] Seeking to harness the power of the Internet and "smart mob" electronic social networks, this challenge will spur development of distributed, bottom-up early warning systems.[98]

However, not all of these efforts need focus on emerging, yet-to-be-developed, or untested technologies. For example, the widespread use of mobile text messaging (SMS) and email before, during, and after the 2004 tsunami suggests that there are unexploited opportunities lying within the capabilities of our existing telecommunications systems. Most importantly, two of the most important innovations in telecommunications in recent years (Figure 1) - the Internet and mobile telephones - play little to no role in formal emergency communications systems.

Figure 1. Growth of New Communications Technologies



[97] Internet Society. "The Internet Rises to the Challenge of Public Warning". [http://www.isoc.org/challenge/]

[98][http://www.stephensonstrategies.com/stories/2004/09/29/10pointPlanToMakeSecurityM.html]

The central challenge to innovation in emergency communications has been that emergency planners tend to see the public as a liability to emergency communications, rather than a resource. As Eli Noam and Harumasa Sato have argued:

> The basic lesson from Kobe is that the usual approach of disaster communications, traditionally based on military-style public safety agencies that are operating in a top-down manner and share information with "civilians" only on a "need-to-know" basis, should be replaced. Instead, we should set up an open-access emergency system - open to inputs from a wide variety of public and private participants and with open to access to that information. Not only would such a system be more efficient as a tool of information and organization, but it would also be more resilient to the shocks of disaster.[99].

Such an approach might rely on both new and old technologies, such as email and the telephone network, but would require a dramatic shift in the role and practices of emergency managers. Rather than executing pre-scripted disaster plans through a military-style command structure, emergency managers would become information managers - gathering and verifying various streams of information and directing it to where it can best be utilized.

Such an approach implies that we should encourage the development of a a wide variety of (even competing) communications channels for emergency use. Yet, for the most part, current efforts in the United States emphasize centralization and standardization. In contrast to current efforts to develop unified "all hazards" networks, this approach may suggest a decentralized approach to emergency communications.

To better understand how to leverage new communications technologies and practices in emergencies, the following questions must be addressed:

Research Questions:

- How are ad hoc communications structures developed in disasters? What can they teach us about improving design for official systems?

---

[99] Noam and Sato, Ibid.

- How does the growing body of research on social network structures, and the way new communications pathways are forming on the Internet, inform the design of future emergency communications systems?
- How do new communications technologies perform in comparison to older more established one during disasters? What can be done to improve their resiliency?

4. Risk Management, Telecommunications and Urban Decentralization

Following the collapse of the Twin Towers, experts questioned the future viability of urban centers in an age of heightened terrorist threats.[100] While there have been no subsequent domestic terrorist attacks in the United States, the threat of such an event is creating powerful incentives to decentralize and scatter commercial activities from central business districts and landmark buildings. Further research is needed to understand how firms are employing new communications technologies to support new locational strategies that seek to manage these risks.

The collapse of the terrorism insurance industry after September 11 has been a key force driving the development of new real estate management strategies. Re-insurers and insurers began "shedding their exposure to terrorism risk" quickly, and as a result "limited coverage for terrorism-related losses is currently available at very high rates, full coverage is often not available at any price, forcing larger commercial policyholders to operate with little or no coverage for such risks... This condition appears to be particularly acute for properties located in central business districts of major metropolitan areas."[101]

One way to manage these risks is through decentralization of facilities and staff, especially in large corporations. A whole array of telecommunications technologies, from video-conferencing[102] to Voice over Internet Protocol (VoIP) telephone service, are being packaged by vendors like Cisco, IBM and others to support this scattering of functions.

However, very little is known about how this process is unfolding, and its impacts. Therefore, the following questions need to be addressed:

- How are companies employing new telecommunications technologies to scatter facilities? Is this a widespread practice? Is it temporary or a long-term commitment?

---

[100] J Kotkin and F Siegel. October 14, 2001. "Terrorism: attacks threaten future of cities" *Los Angeles Times*.

[101] R J Hillman. February 27, 2002. "Terrorism Insurance: Rising Uninsured Exposure to Attacks Heightens Potential Economic Vulnerabilities" (General Accounting Office: Washington, DC)

[102] Wainhouse Research. September 4, 2002. "Wainhouse Research Survey of Business Travelers Tracks Use of Collaboration Technologies". [http://www.wainhouse.com/prtravhab0902.html]

- Is risk-based decentralization actually making the economy more resilient to the disruptions caused by disasters?
- Are the telecommunications networks that support risk-based decentralization more resistant to the types of failures seen in past disasters - physical destruction, congestion, and failure of supporting infrastructure?
- What are the long-term economic tradeoffs between risk-lessening decentralization and the productivity advantages of urban agglomerations?
- What are the lessons for the siting and management of public sector facilities?

5. Rethinking Public Warning Systems

The complete lack of public warning in the 2004 tsunami disaster, and the catastrophic damage and loss of life that resulted, demonstrated the importance of building and maintaining effective public warning systems. The 9/11 Commission repeatedly has noted that available public warning systems in the United States were not effectively utilized during the response to the terrorist attacks in New York and Washington.

In the United States, state and local governments rely upon the Emergency Alert System as their primary mechanism for providing warning information to the public. Designed during the Cold War for presidential use to warn of a nuclear attack, this system has never been activated by any federal agency. Instead, it is extensively used by local governments for weather-related hazards and other emergencies such as chemical spills. However, broadcasters' participation in disseminating these warnings from state and local authorities is on a strictly voluntary basis.[103] However, local governments such as New York City have begun demanding more concessions and control over programming interruptions from broadcasters as they revamp aging systems.

Recent surveys have focused attention on the mismatches between the mission, actual use, and future needs of public warning and the EAS.[104] The Federal Communications Commission recently completed an information gathering process aimed at new regulation for overhauling EAS.[105] However, further research is needed to understand the mismatch between the public warning needs of urban governments and the capabilities of EAS and emerging technologies and practices.

Research needs include:

- How effective are voluntary emergency alert systems at conveying information to the public about emergency warnings and responses? Would mandatory-carry agreements work better?

---

[103] While moot - because it has never been used in the 50-year history of the system - broadcasters are required to carry warnings issued by federal authorities.

[104] Partnership for Public Warning. May 16, 2003. "A National Strategy for Integrated Public Warning Policy and Capability". (Washington, DC)

[105] FCC Docket. No. 04-189

- How can warnings be more effectively targeted at the local level using various types of filters?
- How effective are opt-in email and SMS alerts that have been deployed in various communities around the country (Arlington, VA is one example)?
- How do people access, digest, and act upon official warnings and response instructions? How can messages be designed to improve their effectiveness across a wide range of users?
- What can be done to create an environment for innovative experiments in different communities in public warning systems?

6. *Modernizing the Amateur Radio Service*

Amateur radio enthusiasts provide critical voice communications to FEMA, local emergency response agencies, and the Red Cross in disaster areas throughout the world. However, as the nature of disaster management changes in the 21st century, communications needs are changing as well, and amateur radio is struggling to keep pace. Most importantly, the increased demand for broadband data communications by emergency responders is rendering amateur radio obsolete in all but the most basic survival situations.

However, the ham community is a tremendous disaster communications resource due to its deep and long-standing commitment to publics service, its highly organized internal structure, and its technical knowledge base. The barriers to increasing communications capability largely stem from the way amateur radio spectrum is regulated.

The Department of Homeland Security has called amateur radio operators the "first of the first responders"[106] yet there are no programs or funding sources dedicated to modernizing the services provided by hams in disaster response efforts.

Therefore, the following questions need to be studied further:

- What are the regulatory and technical barriers to innovations in data communications in amateur radio, especially disaster communications?
- How can the amateur radio emergency service link to the growing hobbyist and community network movement around unlicensed wireless technologies such as Wi-Fi, which offer much great data transmission capabilities?
- How can amateur radio volunteers be better utilized within Citizen Corps and other local citizen preparedness programs?

---

[106] "Amateurs 'First of the First Responders,' DHS Official Says". *The ARRL Letter.* Vol. 22, No. 26 June 27, 2003

Acknowledgments

This research was made possible by a grant from New York University's Center for Catastrophe Preparedness and Response.

For more information, please visit http://www.nyu.edu/ccpr/