Communications Infrastructure – Systems and Technology Innovation

Thread Organizer: Eric N. Barnhart, P.E.
Principal Research Engineer and Division Chief,
Communications and Networking Division
Information Technology and Telecommunications Laboratory,
Georgia Tech Research Institute

This white paper addresses the challenges in rebuilding communications infrastructure and service platforms in the New Orleans region following the devastation of Hurricane Katrina. As the rebuilding continues, we must pay attention to lessons learned that are extensible to other locations where resilient, survivable communications infrastructure is imperative. The communications infrastructure in any region is vital to support the economy and civil services at all times and to coordinate mitigation, management, and response in times of disaster. The New Orleans / Gulf region is no exception.

With this dual criticality in mind, we focus on the rebuilding, development and operation of sustainable, survivable infrastructure to meet both needs. We will not focus specifically on stop-gap approaches to providing temporary communications infrastructure to augment that fraction of the permanent infrastructure and services that remained after the storm and flood as much as we will focus on characterizing the "health" of the communications infrastructure after the event, plans for rebuilding, progress, and lessons learned toward increasing sustainability and survivability. The core issue is starkly represented here:

*"The sheer force of Hurricane Katrina disabled many of the communications systems that state and local authorities and first responders rely upon to communicate with each other and with FEMA. This was not an issue of interoperability, **but of basic operability**, resulting from wind, flooding, loss of power, and other damage to infrastructure."*

Michael Chertoff, Secretary, U.S. Department of Homeland Security, Select Committee Hearing, October 19, 2005 (emphasis added).[i]

FEMA

As the photo and quote convey, the core issue is the resilience and sustainability of the basic operability of communications to aid in response, recovery, and function of the economic, community, and public health systems. While interoperability of public safety, national guard and military communications at local, state and federal levels is a key goal nationwide, interoperability cannot be supported without basic functionality in wireless and wired communication systems and services.

The communications infrastructure in the New Orleans / Gulf region suffered heavy damage from Katrina and the flooding that followed. Below, we will highlight some of the effects of the storm on the communications infrastructure, review the interdependencies among critical infrastructure elements, consider the potential of a more robust infrastructure for communications, examine elements of continuity of operations and the relationships between key processes and communications infrastructure, address the roles of regulations and standards, and pose some questions to aid in examination of key issues regarding communications infrastructure in the wake of Katrina.

Effects of the Storm and Flooding

A few statistics illustrate the degree of damage to the communications infrastructure in the New Orleans / Gulf region:[ii]

- In Louisiana, Mississippi and Alabama, service on more than one million telephone subscriber lines was disrupted, with more than 250,000 remaining out of service four weeks after landfall of Katrina.

- More than 35 emergency management-911 call centers were affected, with two call centers in Louisiana remaining out of service four weeks after the storm.

- Infrastructure supporting wireless communication was damaged, with more than 1500 cell sites affected and several hundred remaining out of service four weeks after landfall.

- Only four of 41 broadcast radio stations in New Orleans and surrounding areas remained on the air through the storm and immediate aftermath.

Speakers in the Communications Thread of the Forum will provide additional illustrations of the impact of the storm and flood on wireless, telephony, optical, and hybrid fiber-cable communications plants, and address rebuilding plans and progress.

Interdependencies in Infrastructure

Interdependencies among infrastructure elements that are not part of the physical communication plant *per se* are nonetheless important to recognize, as are the interdependencies among elements of the communications infrastructure itself. These interdependencies have an impact on the survival and operability of the communications infrastructure and on the efficiency and effectiveness of recovery and rebuilding efforts.

Interdependencies within the communications infrastructure can be illustrated by considering the common method for backhaul of wireless traffic for connection to the non-wireless portion of the communications network. This backhaul function is typically implemented by constructing wired links between cell sites, switching centers and other network "points of presence," or PoPs. As a result, even if a cell site is operable, if its

connection to a switching center or to the rest of the switched network is inoperable, the wireless service will be essentially inoperable. This situation arose many times during and after Katrina.

For example, Verizon Wireless experienced service interruptions due to a number of effects, including this one. Before Katrina, Verizon maintained two major switching centers in Baton Rouge and Covington, Louisiana. As a result of Katrina, the Covington facility was isolated from some of the cell sites it normally served due to a break in a fiber-optic communication line operated by another carrier that was damaged. This outage occurred in spite of good design practice implemented by the terrestrial carrier: the fiber-optic ring configuration provides protection against failure by providing redundant physical paths, so that if the ring is cut in one place the service can survive. However, in Katrina, even the redundant path was destroyed. One section of the fiber ring was damaged by the failure of a bridge which the fiber traversed. This example illustrates the interdependency between the communications infrastructure and transportation infrastructure.[iii]

Other examples of the interdependency between communication and other infrastructure abound. One such example is the loss of operability of communications not due to damage to network elements, but to a loss of power. In the commercial wireless infrastructure, some cell sites have backup power in the form of generators, and some do not. Operation of the generators in some cases was degraded or prevented due to damage or flooding. In cases where generators are present and operable, they must be re-fueled to maintain operation. Refueling depends upon passable transportation routes to the generator locations. The importance of power as an underpinning resource in communications is underscored here:

> *"The power system is the foundation on which today's legacy and emerging next-generation communications networks are built, and the reliability of the power system has a more direct and significant impact on communications reliability than any other factor."* [iv]

Interdependencies have impact not only during the rescue and recovery stages following a disaster, but also during the rebuilding phase. For example, underground runs of fiber or coaxial cable may be done in localized areas in rights of way in a very short period of time. However, planning for road reconstruction and execution of the effort may take longer. If the sequence of efforts is such that the buried cable work precedes major work on roadways in the same right of way, destruction of the newly-placed cable may result. These sequencing issues may be driven by market realities in ways that are different from road improvements or communication infrastructure improvements under "normal" circumstances.

Coordination of rebuilding efforts is key to maximizing the economic efficiency of the rebuilding process. Quite simply, the volume of parallel activity in the recovery and rebuilding process far exceeds the volume that can be easily accommodated by affected government agencies and their coordination processes. This situation is exacerbated by

reductions in personnel and their ability to communicate effectively, as was the case with Katrina. This excerpt from a carrier website dealing with Hurricane Wilma illustrates the problem:

> *"As BellSouth continues to make progress in restoring service to customers affected by Hurricane Wilma, some of this work is being unintentionally reversed as underground cables and other telecommunications equipment is damaged in the course of storm clean-up by residents and contractors."* [v]

It is clear that communications infrastructure cannot be considered in isolation from other critical infrastructure elements either in design of solutions or in recovery and rebuilding of plant elements after a disaster.

The Possibility of a More Robust Infrastructure

As timeframes became known for near-complete restoration and rebuild of communications infrastructure in the New Orleans / Gulf region to the level of functionality that pre-dated Katrina, speculation about development of a nationwide "fault-tolerant" communication network arose. Of course, existing systems and infrastructure are fault-tolerant to a great degree, but there are vulnerabilities intrinsic to any system. When contemplating a more robust communications capability, broad questions arise: To what degree should "hardening" of the infrastructure be done? What is the cost? Who would bear the cost? What functions should be supported? Public safety and emergency management centers? Avenues for dissemination of information to the public? Mobile services? Fixed services?

There are some obvious realities to consider as well: Any infrastructure present in the geographic area in which disaster strikes is subject to potential damage and failure. No solution is going to be 100 percent "fail-safe." Only solutions that would involve the ingress of all components of the solution after the event would be immune to this risk. Moreover, as the evolution of the communication fabric in the U.S. and worldwide over the past few decades has shown, any solution crafted and then not used in a real event for several years would likely suffer from a capacity constraint because of the steady increase in communications traffic over time. This is a scalability issue, which is particularly applicable to solutions that do not require any "wired" network segments whatsoever.

In spite of these questions, technology and systems solutions are emerging in the marketplace that offer some hope of rapidly providing some communication capacity in some areas for some users. Wireless internet (Wi-Fi) solutions and voice over IP (VoIP) services can be deployed in combination with satellite connectivity as some approaches in the recovery process illustrated. Other solutions are generally described as "mesh networks" because subscriber and backhaul/backbone traffic flow over the same physical paths, and the wireless networks of nodes typically allow the introduction of new nodes in the network on an *ad-hoc* basis without significant re-design of connectivity paths. To date, much more emphasis has been placed on developing regional and national

interoperability in public safety systems for simple voice communications than on solutions to support a broader range of communications options such as data and video communications.

Still other emerging communications technologies, such as "software" or "cognitive" radio systems that will allow adaptation of communication methods with changes in location, spectrum usage and information flow demands are coming, but wide adoption of these methods is still in the future. John Powell, senior consulting engineer with the National Public Safety Telecommunications Council, comments that "packet, mesh and cognitive (radio) aren't really on the agenda yet for public safety networks."[vi] For the short term, these are trends to keep an eye on. It must be acknowledged, however, that even if such solutions are deployed, power remains an issue.

In summary, issues surrounding a "more robust" infrastructure tend to fall into one of two categories: (1) improving the robustness or survivability of infrastructure to support communications systems and approaches that pre-dated Katrina from the standpoint of functionality, and (2) deployment of fundamentally "new" approaches that exploit infrastructure in a different way. The reality is that solutions for the long term will likely consist of a mix of these two approaches.

Continuity of Operations - Processes and Applications "Behind the Network"

Communication networks are clearly critical infrastructure, but why? Just as transportation routes are important because they allow the movement of people and materials, communication networks are important because they enable applications and processes – the networks are a means to an end, and not the end themselves. Networks are viewed as critical infrastructure because enterprises (whether government, commercial, community or non-profit) are focused on continuity of operations and disaster recovery with their applications and processes in mind, not the networks themselves. Survivable, resilient networks are an enabler of *continuity* of operations and a minimizer of the time required for *recovery* of operations.

Viewed from the enterprise perspective, design approaches for continuity and recovery typically fall into one of two categories: (1) replication and failover (for continuity) and (2) backup and restore (for recovery). Redundant systems (replication) and rapid switchover when needed (failover) both contribute directly to continuity. Maintenance of up-to-date system information in more than one place (backup) and methods to re-start systems (restore) both contribute directly to recovery. To benchmark systems for continuity and recovery performance, two types of design goals commonly applied – recovery time objective and recovery point objective. Note that these terms both address recovery and not continuity. This is an acknowledgement that no practical, complex system is 100% fail-safe, and that practical measures addressing continuity focus on minimizing loss of functionality and loss of "downtime." Operational processes often can tolerate small interruptions of service in underlying infrastructure, so continuity is driven by minimizing the duration of outages and recovery time.

Recovery time is the amount of time required to re-establish a particular class of service. Obviously, the nearer to zero one can drive the recovery time, the better. R*ecovery time objective* defines the maximum acceptable time to re-establish service. *Recovery point objective* defines the degree to which it is acceptable to lose state or status information regarding the operation of a system or process. For example, if the recovery point objective is 4 hours, it is defined as acceptable to lose all state information for the 4 hours immediately preceding failure if there is a system failure.

The recovery point objective in an information-based system drives periodic data backup processes. Typically, smaller recovery point objectives mean more intensive data backup processes and more consumption of network, computing, and storage resources to accommodate the more-intensive backup process. With limited resources, consumption for backup or data replication processes leads directly to degraded capacity for real-time operation. Performance and price considerations for network-connected storage media are obviously central to recovery time and recovery point questions. Enterprises face difficult tradeoffs of cost, complexity, and performance relative to continuity and recovery issues. For example, the State of Louisiana currently has two data centers to provide replication, but both are in Baton Rouge. The State is examining steps to provide backup at a point further north in the State with a possible, permanent location in the northern region of the State.[vii]

Communications service providers in the New Orleans / Gulf region have acted aggressively over the last year to improve performance to support continuity and recovery, as a few examples from the wireless community illustrate. The City of New Orleans is planning and implementing new mobile network operations centers and municipal Wi-Fi capability. In 2006, Cingular Wireless is investing $1.8 billion to improve network coverage in the Southeast U.S., adding additional generators and new mobile access command headquarters. Sprint Nextel is purchasing additional generators and satellite-connected portable cell sites. Verizon indicates that about 90 percent of cell sites in areas susceptible to hurricane damage have on-site backup generators. Finally, T-Mobile has redesigned generators using liquid propane fuel for extended operation.[viii] In summary here, it is important to remember that continuity and recovery of operations is a core consideration that drives decisions about the detailed design of communications infrastructure.

Roles of Standards and Regulations in an Era of Deregulation and Competition

The deregulation of telecommunications markets in the past three decades has had an impact on the ability of standards and regulatory bodies to impose requirements on the operators of communication systems. This is largely true in public-sector and utility systems as well as commercial systems. If deregulation has allowed the proliferation of more numerous, heterogeneous options for system implementation while recent events have underscored the need for increased resiliency, survivability and interoperability, then what can be done to ensure the then needed robustness?

The answer depends on the type of infrastructure under consideration, the source of the funding for it, and the regulatory domain imposed on it. Here, a distinction can be drawn between public-sector/utility systems and commercial systems. Consider public-safety radio communication systems versus commercial cellular systems as an example. Public–safety and utility wireless systems typically are smaller (measured by number of subscribers or users) and more oriented toward a single purpose than commercial wireless systems. Moreover, their construction and operation are typically funded through taxing authorities at the local, state, or federal level or through collection of utility fees that are regulated at various levels of government. Financing for these systems may flow between levels of government, allowing the source of funding to impose performance requirements on the systems acquired through these funding mechanisms.

The impact of limited-scope systems is captured by this observation:

> *"Most utilities, regardless of service territory size or proximity to the centers of the storms, reported that their communications systems stood up well to the hurricanes. This stands in stark contrast to the public switched network (PSTN) in the region and wireless carriers, who suffered extensive loss of service and slow recovery time. The comparison points to the fact that communications systems, if built extremely well, can withstand the intense wind and/or flooding associated with these events; however, unlike public networks, CII (critical infrastructure industries) systems' redundancies and robustness can be limited in size and scope, since they are designed and constructed to meet the specialized needs of a single entity or group of companies. Such construction would be cost-prohibitive for a commercial system designed to serve millions of the general public."* [ix]

It is clear that large-scale, commercial communications systems must face tradeoffs that limited-scope systems can treat in a different way. The market realities behind these tradeoffs cannot be ignored. Investment in survivability that drives the cost of service outside competitive ranges is not in the interest of any stakeholder since such a condition would result in elimination of the service from the marketplace. Finding the balance point between functionality and market sustainability is clearly a key challenge in today's competitive communications marketplace.

Nonetheless, when infrastructure is procured, the procuring entity can always impose operability and functionality requirements as conditions in the Request for Proposal or other procurement processes. Additionally, use of the public spectrum resource, under license from the Federal Communications Commission, or use of the public right of way for transmission both allow definition of performance requirements to some degree. Requirements, recommendations and standards for communications infrastructure are myriad across the various levels of government and in the commercial market. Examples include the National Communication System (NCS), first established by President Kennedy and expanded during the Reagan administration to address coordination across 23 federal departments and agencies; the National Public Safety Telecommunications Council (NPSTC), including its Public Safety Wireless Advisory Committee (PSWAC);

the FCC Public Safety National Coordination Committee (NCC); Title 47 of the Code of Federal Regulations (FCC Rules); the American National Standards Institute (ANSI); the Institute of Electrical and Electronics Engineers (IEEE), the Telecommunications Industry Association (TIA); Cable Laboratories; the Network Equipment Building Standards (NEBS); the Open Mobile Alliance (OMA); and the International Telecommunication Union (ITU). Coordination among these various agencies and organizations, and their membership, is a daunting challenge, but the challenge must be met to ensure the widespread adoption of best practices.

Questions to Consider in the Forum

In the Communications Thread of the Forum, we will learn about details of damage to the hybrid fiber/co-axial plant, the public switched network, copper plant, switching centers, and infrastructure supporting wireless communications. Speakers will address the planning and logistics of the rebuilding effort over the past year. Issues pertaining to coordination and interdependencies between critical infrastructure elements will be examined and lessons learned that can be extended to planning for increasing resilience and survivability of critical communications infrastructure will also be reviewed.

As we address these details, questions to consider both within the bounds of communications infrastructure issues and in a cross-disciplinary manner include:

1. What are the limits to "robustness" in communications infrastructure?
2. How is resilience and survivability characterized?
3. How do tradeoffs between design criteria for rare events and everyday, market-driven uses affect decisions about communications infrastructure?
4. What are the trends toward the lofty goal of a completely "fault-tolerant" communication infrastructure? Is this really possible?
5. What new technologies have been put into play given the rebuilding requirements that may not have been made available to the region without Katrina as the driver?
6. How do continuity of operations issues relate to recovery issues? One idea suggests the network "never goes down" while the other suggests that it will, but we should recover "quickly."
7. How do we reconcile questions about interoperability versus basic operability? What are the priorities? How do they relate?
8. What about 'standards"? Who enforces them? In what segments of the market are they appropriate?
9. How do decisions get made about what to rebuild quickly as opposed to what elements of the communication infrastructure must wait for cues from re-population patterns and the re-initiation of economic activity?
10. With new investment in the New Orleans / Gulf region, what design/deployment lessons learned can be captured and re-applied?
11. What are the best ways to capture, characterize, and disseminate this new knowledge?

[i] *A Failure of Initiative*, Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina, U.S. House of Representatives Report No. 109-377, February 15, 2006.
[ii] Ibid.
[iii] Jackson, Joab, "Telecom Infrastructure No Match For Katrina," *Washington Technology*, November 7, 2005.
[iv] Rauscher, Karl; Rick Krock; Jim Runyon: and Peter Hayden, *Intrinsic Vulnerabilities of the Power Systems Supporting Communication Networks and Expert Strategies for Defense,"* Lucent Technologies Report, March 30, 2006.
[v] "BellSouth's Hurricane Recovery Efforts" at bellsouth.com/community/hurricane/index.html image dated March, 14, 2006.
[vi] Wirbel, Loring, "Authorities Blamed for Communications Networks' Failure Under Katrina's Attack," *EE Times*, September 5, 2005.
[vii] "State of Recovery," *Washington Technology*, June 26, 2006.
[viii] Alleven, Monica, "Carriers Batten Down the Hatches," *Wireless Week*, July 15, 2006.
[ix] *Hurricanes of 2005: Performance of Gulf Coast Critical Infrastructure Communications Networks*, Report of the United Telecom Council, Washington, D.C., November, 2005.