Transformation for Disaster Relief

Developing a Hastily Formed Network During Operation *Vigilant Relief*

Case Studies in National Security Transformation
Number 2
John M. Epperly
December 2006

Sponsored by the Office of the Deputy Assistant Secretary of Defense
Forces Transformation and Resources

Prepared by the Center for Technology and National Security Policy

The views expressed in this article are those of the author and do not reflect the official policy or position of the National Defense University, the Department of Defense, the Virginia Army National Guard or the U.S. Government. All information and sources for this paper were drawn from unclassified materials.

LTC John M. Epperly is currently the battalion commander for 3-116th Infantry, 1st Brigade Combat Team, 29th Infantry Division (Light), Virginia Army National Guard. He commanded 2-116 Infantry during Operation *Vigilant Relief* in Mississippi in the wake of Hurricane Katrina. LTC Epperly is a 1989 graduate of the United States Military Academy at West Point, NY, and holds an MBA in Finance from Drexel University. He served several tours on active duty as an armor and cavalry officer, primarily with 10th Cavalry and 70th Armor. In his civilian role, he is the general manager of Innovative Concepts, Inc., a wholly owned subsidiary of Herley Industries, Inc. Innovative Concepts is an embedded software systems company that provides datalink communications to the U.S. military and first responder community, as well as numerous international clients.

Introduction

The purpose of this case study is to facilitate the analysis of the role and effects of network-centric operations during the National Guard's initial response to Hurricane Katrina, which made landfall in Louisiana August 29, 2005. The study explores the problem of establishing a hastily formed network during a complex humanitarian disaster scenario by focusing on the difficulties of establishing a network at the rifle battalion level during Operation *Vigilant Relief*. In particular, the study focuses on those operations along the Mississippi Gulf Coast between September 6 and October 1, 2005 conducted by the Virginia Army National Guard's 2nd Battalion, 116th Infantry, part of the 1st Brigade Combat Team of the 29th Infantry Division (Light). 2-116th Infantry was designated as Task Force (TF) Stonewall prior to its deployment to Mississippi. A sister National Guard task force from Virginia designated TF *Cardinal* was deployed simultaneously to the Louisiana area of operations (AO). While both units eventually established operational networks, the initial stages offer valuable lessons on what to expect during a complex humanitarian disaster (CHD)—especially in terms of communication networks and the attendant effect on continuity of operations. By reviewing the case study, future policymakers as well as civilian and military leadership will have a better frame of reference for solving communication problems encountered during a CHD and also potential solutions for similar incidents.

Strategic Situation, Background, and Event Significance

On August 27, 2005, two days before Hurricane Katrina made landfall on the U.S. Gulf Coast, President Bush declared a state of emergency for Louisiana, Mississippi, and Alabama. The resulting evacuation orders from local and state authorities affected over one million people, many in hard to access rural areas. Prior to landfall, 4,000 National Guard soldiers had been pre-positioned in Louisiana and 2,500 in Mississippi to shorten response time. [1] Despite the precautionary measures, many troops were not available when needed. Significant portions of the 155th Brigade Combat Team from Mississippi and 256th Brigade Combat Team from Louisiana were deployed to Iraq when Katrina struck. This reduced the number of troops available to the governors of those heavily damaged states.[2] While the states were left with fewer home units, several Emergency Management Assistance Compacts (EMACs) were in place between most of the Gulf Coast states. The EMACs were essentially mutual aid agreements between the state governors allowing the National Guard assets from one state to be used in another state

[1] LTG H. Steven Blum Interview, "Defense Department Briefing on Ongoing National Guard Response to Hurricane Katrina Transcript," September 3, 2005. Available online at <http://www.dod.mil/transcripts/2005/tr20050903-3850.html>.

[2] Government Accounting Office, "Hurricane Katrina: Better Plans and Exercises Need to Guide the Military's Response to Catastrophic Natural Disasters," GAO Report GAO-06-808T. Statement for the Record to the Subcommittee on Terrorism, Unconventional Threats and Capabilities, Committee on Armed Services, House of Representatives, May 25, 2006, 7.

without federalization.[3] These EMACs allowed for rapid reinforcement of National Guard units in Mississippi and Louisiana by units in contiguous states. Unfortunately, most non-contiguous states did not have EMACs established with Mississippi and Louisiana. Previous disasters, including Hurricane Camille, had been handled by the combined efforts of Gulf Coast states with occasional federal assistance. Katrina, of course, was different. Due to the scale of the Katrina disaster and the required response, EMACs eventually were developed with every state in the union to allow units from all states to participate in the incident response. Such an EMAC allowed my battalion (2-116th Infantry) to be deployed from Virginia to the Mississippi AO.

At 0600 Eastern Daylight Time (EDT) August 29, 2005, Hurricane Katrina made landfall on the Gulf Coast of the United States near Buras-Triumph, Louisiana. It was the strongest Gulf hurricane and the fourth-strongest Atlantic hurricane recorded to that date, and the deadliest storm to affect the U.S. mainland since 1928. Katrina may have been the largest hurricane of its strength to approach the United States in recorded history; it caused devastation over 100 miles from the storm center.[4]

The effects of the hurricane were horrific. Many of the levees protecting New Orleans were breached and the city flooded, and the city was completely incapacitated from the resulting turmoil and flood damage. Beyond the city, nearly 200 miles of coastline were devastated in three states. Katrina caused roughly $75 billion in damages (in 2005 dollars), making it the most costly hurricane in U.S. history. Additionally, Hurricane Katrina was blamed for 1,836 deaths in the affected region.[5] To deal with this event, the National Guard eventually deployed more than 50,000 troops from 49 states and four territories in a little over three weeks, not to mention thousands of tons of supplies.[6] The response was the largest domestic deployment of the National Guard in U.S. history.

TF Stonewall Deploys

My unit, 2-116th Infantry, was put on alert at 8 p.m. EDT, Saturday, September 3, 2005, over the Labor Day weekend. The alert was sent from the Virginia National Guard Joint Operation Center (JOC) at Fort Pickett, Virginia, to all affected units notifying us to prepare for a possible deployment. The alert effectively functioned as a warning, allowing units to prepare for mobilization. The alert also gave us the general parameters of the mission we would likely receive. This information was distributed in what is called a Warning Order (WARNO). The alert was preceded by the initial development of an EMAC between Virginia and Mississippi, which meant that Mississippi was agreeing to fund the Virginia troops … at least initially. The alert was followed by mobilization

[3] FEMA, "Emergency Management Assistance Compact (EMAC) Operations," Final Pre-Course Reading Assignment. FEMA Emergency Management Institute, May 2005, 1-2. Available online at <http://training.fema.gov/EMIweb/downloads/EMAC_Full_Precourse_04_14_05.pdf>.
[4] Wikipedia, "Hurricane Katrina," 2005. Available online at <http://en.wikipedia.org/wiki/Hurricane_Katrina>.
[5] Ibid.
[6] Lou Dolinar, "Katrina: What the Media Missed," *Real Clear Politics*, May 23, 2006. Available online at <http://www.realclearpolitics.com/articles/2006/05/katrina_what_the_media_missed.html>.

orders at 4 p.m. EDT Sunday, September 4, which allowed for a recall of troops into local armories.[7] The deployment order called for a troop and equipment tasking of 250 Virginia Guardsmen and 34 vehicles of varying types.[8] The order also called for the main body of troops to deploy by air no later than 3 p.m. EDT September 6. The ground vehicle convoy was to conduct a 1,300 mile road march and conduct a link-up with the main body at Camp Shelby in Mississippi.[9]

The advance party arrived by air in Jackson, Mississippi, September 6 at 11 a.m. EDT, 43 hours after mobilization, with roughly two tons of supplies and equipment. The main body arrived some seven hours later.[10] Upon arrival, the task force was assigned to the 38th Infantry Division of the Indiana Army National Guard, which had tactical control of all relief operations along the Mississippi Gulf Coast and was subordinate to the Mississippi National Guard Joint Operations Center (JOC), which in turn was subordinate to the Mississippi Emergency Management Agency (MEMA).

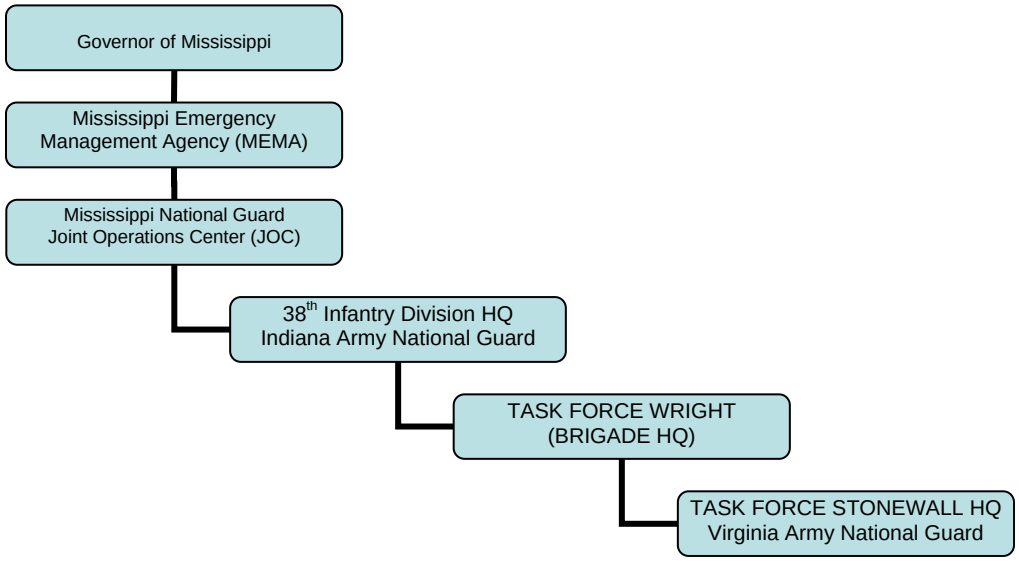
Figure 1 shows the command relationship. The distinctions are important. While National Guard units remained under state control, the chain of command for active forces, such as the 82nd Airborne Division, culminated with U.S. Northern Command (NORTHCOM). Thus, two separate chains of command were in effect for active and Guard forces, because guard forces were not federalized. Throughout the Katrina relief operations, National Guard forces remained in a Title 32 status, that is, under the control of the state governors. While the Federal Government was paying for the incident response, it stopped short of federalizing National Guard soldiers under Title 10.[11]

This distinction is important because Guardsman in either a state active duty status or Title 32 status *can* be used for law enforcement activities, whereas active duty soldiers are prohibited from law enforcement because of Posse Comitatus restrictions.[12] When soldiers from one state are used for law enforcement in another state, an agreement between the state attorneys general must be developed. It took approximately 48 hours for the attorney general of Virginia to conclude an agreement with the attorney generals of Louisiana and Mississippi. Shortly after arrival, TF Stonewall was reinforced with an additional infantry company from the 76th Infantry Brigade, Indiana Army National Guard, and a Military Police Platoon, also from Indiana Army National Guard. This brought the total strength of TF Stonewall to 410 soldiers and 68 vehicles.[13]

---

[7] 2-116th Infantry Daily Staff Journal, DA Form 1594, September 4, 2005, 1.
[8] The vehicles deployed in TF Stonewall included numerous types of HMMWVs, 2 ½ ton capacity cargo trucks, 5 ton capacity cargo trucks, HMMWV ambulances, a 5-ton capacity wrecker, and several trailers for carrying cargo and large generators.
[9] 2-116th Infantry Operations Order 05-09, Para. 3.e. Coordinating Instructions, September 4, 2005, 3.
[10] 2-116th Infantry Daily Staff Journal, DA Form 1594, September 4, 2005, 4.
[11] Under Title 10, Guard soldiers work for the President of the United States and share the same chain of command as their active duty counterparts. Guardsmen who have been federalized under Title 10 are subject to the Posse Comitatus Act and cannot be used for law enforcement within U.S. borders.
[12] Lawrence Kapp, "Reserve Component Personnel Issues: Questions and Answers," *Congressional Research Service*, Order Code RL30802, January 18, 2006 (Washington DC: U.S. Government Printing Office), 10.
[13] 2-116th Infantry Fragmentary Order 2 to Operations Order 05-09 Para. 1b, Friendly Forces, September 12, 2005, 1.

Figure 1. National Guard Chain of Command



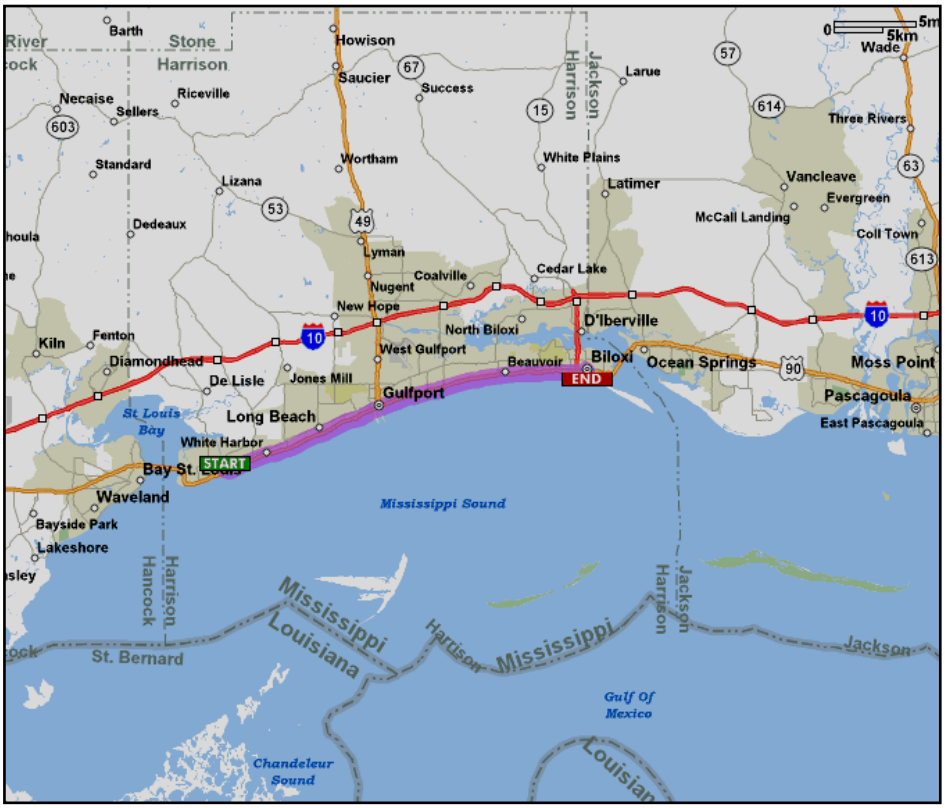
[14]

TF Stonewall AO

After the task force linked up with its ground convoy September 8, it was immediately tasked with providing security, humanitarian relief, and recovery assistance to four Mississippi Gulf Coast towns: Pass Christian, Long Beach, Gulfport, and Biloxi. The task force frontage was 22 miles wide with a 10-mile inland depth—a very large area for a unit this size. Figure 2 shows the battalion task force AO. The terrain in the AO is only a few feet above sea level, with many water obstacles due to flooding and many streambeds. In addition, much of the AO was urban, with significant damage to structures. Many bridges and roads were either unsafe to use or destroyed outright. Highway 90 along the beach was nearly destroyed and too dangerous to use, with the exception of emergency vehicles. Rubble and storm debris often impeded vehicular movement. The weather was generally hot and humid, as is to be expected along the Gulf Coast in September. Electrical storms were common, but rainfall was not.

[14] The command relationship shown in figure 1 does not show that the Virginia JOC exercised *administrative control* of TF Stonewall during Operation *Vigilant Relief*. Thus, the Virginia command team exercised limited authority over TF Stonewall and assisted the task force in solving soldier problems while deployed. However, in terms of day-to-day operations, the 38th Infantry Division and Task Force maintained *tactical control* of TF Stonewall, as shown in figure 1.

Figure 2. Battalion Task Force AO[15]



TF Stonewall Mission and Key Tasks

The TF mission statement read:

> Task Force Stonewall deploys to the Mississippi Gulf Coast region no later than 061500SEP05 and conducts humanitarian relief, recovery and security operations vicinity Gulfport and Biloxi, MS in order to assist civil authorities in restoring those communities from Hurricane Katrina.[16]

The Operations Order (OPORD) for deployment delineated the first three key tasks based on the battalion commander's intent:

- Provide security in sector
- Provide humanitarian assistance
- Provide support to recovery operations[17]

[15] Mapquest. Available online at <www.mapquest.com>.
[16] 2-116th Infantry Operations Order 05-09, Para. 2.
[17] Ibid.

Providing *sector security* to such a large sector was a significant task, given the extent of the AO. Specifically, TF Stonewall had to deny unauthorized personnel access to the beach area while recovery operations were underway. This was done by establishing a cordon with 54 static checkpoints manned by two soldiers 24 hours a day. The static cordon was reinforced by roving, dismounted patrols and military police patrols mounted on High Mobility Multipurpose Wheeled Vehicles (HMMWVs). This reinforcement was necessary because of the significant distance between many checkpoints—in many cases up to 600 meters—which sometimes allowed people to slip between the checkpoints. Looting and civil violence were sporadic in the initial 72 hours after the task force arrived. Thereafter, very little violence or looting was reported or seen. Drug-related and gang activity within the Gulfport and Long Beach city limits gave the Red Cross some difficulty, but local law enforcement and the military police from TF Stonewall dealt with it quickly. The task force also provided security to Point of Distribution (POD) sites. The local populace were able to acquire food, water, ice, clothing, and sundry items at several POD sites located throughout the task force AO. These sites were usually run by the American Red Cross or volunteer non-governmental organizations (NGOs), such as church groups.

In addition to sector security, the task force also provided *humanitarian assistance*. While securing POD sites, task force personnel often helped distribute supplies. Further, task force personnel conducted "search and assist" missions by canvassing rural areas in two-man HMMWV teams to ensure that residents needing assistance were identified and, if necessary, rescued. Search and Rescue operations were an implied task for TF Stonewall within the confines of the specified task of providing humanitarian assistance. In fact, most of the search and rescue work within the Mississippi AO was completed by September 9.

Finally, task force personnel provided support to the *recovery* effort by securing power and water utility workers while they worked to restore basic services. The task force also assisted the local populace, where possible, in clearing debris. This was generally done on roadways to ensure vehicular access. Additionally, dismounted patrols assisted recovery operations by identifying and marking human and animal biological remains for later recovery by other agencies, such as the Georgia Bureau of Investigation and Harrison County Animal Control.

The Problem of Creating a Network in a Disaster Area Emerges

By this point, several items have been established: the strategic situation and event significance, the troops and equipment available to TF Stonewall, the task force mission and key tasks, as well as a description of the AO. Establishing a communications network under these conditions with such aggressive mission parameters proved extremely challenging. The problem of creating a network was compounded by the following challenges, which could be grouped into two categories: *technology based* and *policies, techniques, and procedures.*

Technology Based Challenges

The Sheer Size of the AO: TF Stonewall was tasked with providing the aforementioned support in an area measuring 220 square miles with 410 soldiers. Usually, the doctrinal frontage of a sector for a U.S. Army Infantry battalion no more than three kilometers (about two miles), and depth is no more than five kilometers (about three miles), depending on such factors as the mission, terrain, and available troops and equipment. The size of the sector made it very difficult to establish a standard FM radio communications network with the communications equipment normally found in a rifle battalion, such as SINCGARS radios.

Communications Equipment: Communications equipment provided two main challenges. First, there were not enough long range OE-254 antennae to adequately cover the sector with the standard FM communications suite. There were also too few SINCGARS radios because so many checkpoints and dismounted patrols were underway. This problem was exacerbated by the fact that much of the necessary equipment was not available because it had been reassigned to other National Guard units deploying overseas in support of the Global War on Terror. (The second challenge was that much of the communications equipment that was available was not interoperable with other first responders (police, fire, and rescue) or other government agencies. Thus, the traditional communications links to establish a wireless network were insufficient for the task.

Policies, Techniques, and Procedures Based Challenges

Minimal Situational Awareness: The most significant challenge to the problem of developing a working network in the disaster zone was discovering who should be in the network. Upon reaching the AO, situational awareness as to whom and what resources were available was minimal. Nor was there a great deal of information available on the location of these resources. Alternatively, situational awareness of where the military units were located was very good based on the briefing from the 38th Infantry Division's Main Command Post. However, in a domestic support operation (DSO), especially a CHD, it is vital to know the location and capability of other government and civilian relief agencies, because these agencies usually provide the bulk of relief support.[18] Little to no information was available on the disposition, composition, and general condition of local government; police, fire, and rescue; Federal Emergency Management Agency (FEMA) command posts; Red Cross shelters; and power and water recovery teams, to name a few. All of this had to be determined once TF Stonewall arrived on the scene. Because the task force sector straddled four different municipalities and one county, tracking down the information was difficult. Each municipality had a local government, fire department, and police department that needed to be located and liaison established. Finding them all and coordinating consistent communications often proved a challenge. The solution used by the battalion, as discussed later, was decidedly low-tech.

[18] U.S. Department of the Army, FM 3-07 *Stability Operations and Support Operations* (Washington, DC: February 2003), 1–7.

Limited Training in Developing a Network in a Disaster Scenario: TF Stonewall deployed with a command team that had more than 100 years of experience in developing and exercising command and control of widely dispersed units in austere, all weather environments. The U.S. military is uniquely suited and well trained to deploy into environments and scenarios where they must create a working network from scratch using a myriad of communications and command and control techniques. The problem of creating a network during Operation *Vigilant Relief* came when TF Stonewall needed to integrate numerous other organizations and agencies into its normal military network. Compounding the system interoperability problems was the fact that TF Stonewall had never *trained or rehearsed* the integration of these organizations and agencies. Nor had these organizations and agencies trained to integrate with U.S. military units. The battalion task force Standard Operating Procedure (SOP) had little in the way of tactics, techniques, and procedures for developing a hastily formed network with the diverse governmental organizations and agencies also deployed within the assigned sector. TF Stonewall discovered that interagency training and rehearsal is absolutely fundamental to real disaster preparedness.

The Constantly Changing Network: Further exacerbating the complexity of forming a comprehensive network was the existence of large numbers of small, undocumented, NGOs providing relief in the AO. On any given day, numerous church and volunteer groups were providing food and clothing. Some of the groups were well financed and established impressive support operations. Others would arrive in-sector, provide some assistance, and depart within a few days. The task force needed to maintain awareness on who and what organizations were providing support in the AO. Often, Guardsmen on static checkpoints or patrols would encounter people who would ask how and where to get services. Additionally, Guardsmen had to field questions on when it was okay to return to homes and by what route. Thus, it was critical that Guardsmen in the field be kept well informed with the latest information from the network. Interestingly, the Guardsmen on checkpoints and patrol had become a node in the network of everyday Mississippians in the disaster area. Besides the task force tactical operations center (TOC), and perhaps FEMA, no organization or agency was even trying to maintain a common operational picture of the sector. The task force was able to inform the populace about where to get certain services via our 54 static checkpoints and dismounted patrols. Keeping track of the changes within the network was a major daily challenge.

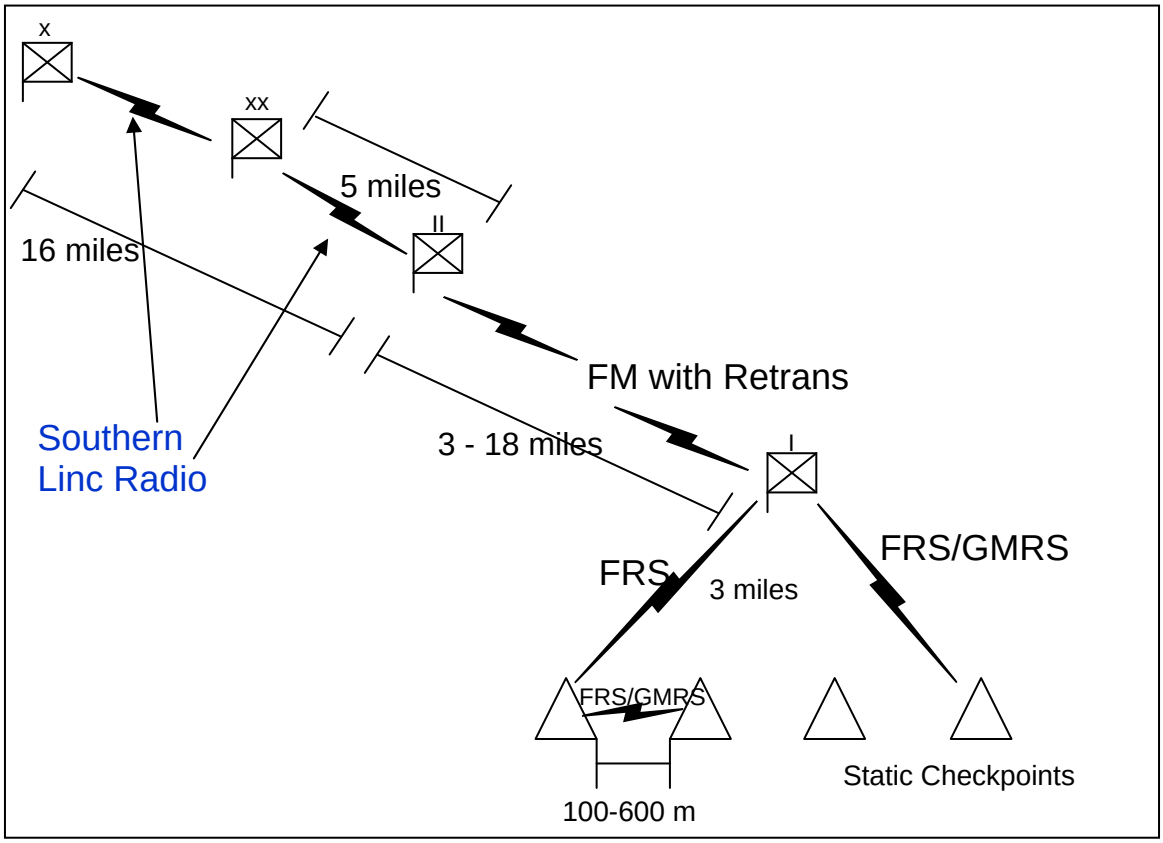
Sewing Confusion—Inconsistency of Policy and Procedures: The sixth challenge to the problem of creating a network in a disaster area is the inconsistency of policies and procedures among townships within the task force sector. *Disasters usually overlap political boundaries, often resulting in a non-uniform response and confusion within the network and with the policies of neighboring jurisdictions.* In the TF Stonewall sector, four townships had policies that often contradicted each other. For example, one of the key tasks for TF Stonewall was to secure the beach areas from extraneous traffic and sightseeing so that emergency workers could do their jobs more effectively. Downed power lines, fetid water, and dangerous wildlife, such as alligators and snakes in places they were not normally found, made for extreme safety issues. Unfortunately, some of the townships were more lenient than others in allowing access to beach areas. Different

policies were aired on local radio stations and enforced by local police departments. This made it very difficult to create and enforce a standard policy via the network. Some localities refused the use of concertina wire, while others allowed it to enable the National Guardsman assigned to their town to do more dismounted roving patrols with fewer static checkpoints. However, when one town used concertina to deny access to the beach area and another town did not, it was easy for people to drive a mile or two, bypass the concertina roadblock, and gain access to restricted areas. Adding to the confusion, local governments often changed policies and access times to the beach areas. Even local police were often confused. Some days access was granted by merely showing a driver's license; other days a driver's license along with a recent utility bill for the address in question were required to show proof of occupancy. In the end, the inconsistency in policy reduced the effectiveness of the response. These inconsistencies created stress on the network and often reduced the credibility of relief agencies while increasing public frustration.

The TF Stonewall Hastily Formed Network—*A* Solution, Not *The* Solution

A network is an interconnected system of things or people and consists of nodes and links. Once the battalion task force arrived on station, we had to identify the nodes in our network and then establish communication links. We identified two types of nodes: military and non-military. The military nodes were simple because they were largely known and we had trained to use them in previous exercises. Examples of military nodes were the task force TOC, company command posts, the 54 static checkpoints throughout the task force sector, and brigade and division headquarters. These military nodes were the same network nodes found in any standard military network. These nodes were often connected by standard FM communications using SINCGARS radios and OE-254 long-range antennae. The FM network links were augmented by cell phones, satellite phones (usually Iridium), and FRS/GMRS handheld radios for shorter communication links. Figure 3 illustrates the basic military nodes and links from the static checkpoints providing the security cordon along the coast line to division headquarters, along with the average distance the network link had to traverse. The Southern Linc radios provided full duplex (two-way) radio capability over a CDMA cellular network. These were only deployed to company commanders and above.

Figure 3. Voice Network from Checkpoint to Division Headquarters



While the military nodes were easier to identify, the non-military nodes were absolutely crucial to mission success because of the services and supplies they provided the populace. FM 3-07 *Stability Operations and Support Operations* points out that interagency cooperation and unity of effort are crucial to mission success.[19] A functioning network is an enabler to that success. To have a network, one must be able to identify the nodes in that network and link them together. Unfortunately, upon the task force's arrival, no one really knew who or what was in our sector, much less what was on its way. Therefore, our mounted and dismounted patrols had to discover these nodes over the first three to four days on station. While this technique was decidedly low-tech, it did work—after a while. However, the time it took greatly reduced the effectiveness of the humanitarian response for all agencies in the intervening period.

One must remember that non-military governmental agencies and NGOs have no network infrastructure equivalent to Blue Force Tracker, which enables a common operating picture to be created rapidly. Even the military nodes did not have an immediate common operating picture at all levels, because most National Guard units were not fielded with the latest digital communications equipment being used in theaters

[19] U.S. Department of the Army, FM 3-07 *Stability Operations and Support Operations* (Washington, DC: February 2003), 1-7.

like Iraq or Afghanistan. Operations *Enduring Freedom* and *Iraqi Freedom* had, in fact, drained a great deal of standard communications equipment from many National Guard units, leaving them less than fully equipped for responding to natural disasters.

Table 1 shows some of the military nodes external to TF Stonewall and some of the non-military nodes in our sector. Once we identified these nodes and met with the leaders running them, we were able to establish communications links in ways which will be discussed later. The key point is that to have both a united and effective effort during CHDs, it is critically important to rapidly establish a network. Otherwise, military units and civilian agencies can wastefully duplicate efforts unknowingly. What's worse, they can inadvertently work at cross purposes. Even once nodes have been established, the work must continue. Identifying nodes is a non-stop process because the network nodes change over time with the arrival and departure of new military units and relief agencies/groups.

Table 1. Military and Non-Military Nodes

Military Nodes	Non-Military Nodes
Mississippi Joint Operations Center	Mississippi State Government
Virginia Joint Operations Center	Municipal Governments of 4 townships
38th Infantry Division HQ	Police Departments of 4 townships
Task Force Wright (Brigade) HQ	Fire and Rescue Departments of 4 townships
Tennessee National Guard (Engineers)	2 American Red Cross Shelters
1-293rd Infantry (Battalion HQ to the east)	Cellular Phone Companies (5 identified)
	Local FEMA Operations Center (Gulfport)
	Georgia Bureau of Investigation (Remains Recovery)
	Indiana State Police (Augmentation to local Police)
	Gulf Power Company
	Gulfport Memorial Hospital
	Biloxi Regional Medical Center
	Local Water Authority
	Church groups and volunteer organizations

Network Links in TF Stonewall's Hastily Formed Network

Once the network nodes were identified, we had to establish network links. We used several means to do this. As previously mentioned, most military nodes were linked with FM communications via SINCGARS radios and OE-254 antennae. In the early hours and days, we actually had to use couriers or liaison officers for the outlying nodes, which literally reduced our communication to World War I methods. Again, this was a very low-tech solution. However, there were advantages to the face-to-face communication the liaison officers used with agencies like the local police departments, the American Red

Cross, and FEMA. The task force probably enjoyed better communication later, when the regular communication links became operational, because this early face-to-face communication established relationships that otherwise might not have existed.

Balanced against the advantage of face-to-face communication was the information lag time caused by the travel time between nodes. Often information is useful only if received in a timely fashion. The lag time associated with travel by liaison officers and couriers often reduced the value of information dramatically. Fortunately, the absolute need for liaisons and couriers was very short lived, because other methods of communications rapidly became available. The cell phone companies were able to restore their networks within days of the disaster. It is worth noting that the cell phone and power companies did a remarkable job in getting their services restored in a timely manner. The cell phone companies in particular demonstrated strong continuity of operations planning (COOP) and execution. They arrived on scene shortly after the storm passed with their own self supporting task force that included replacement equipment and life support, such as tentage, food, water, and power generation for their workers.

While the initial cell phone service restoration left many dead spots, our ability to link nodes improved dramatically. We were able to use cell phones to establish communication with outlying checkpoints and command posts as well as other agencies. In fact, cell phones, and to a lesser extent satellite phones, allowed us to establish links to agencies we could not have communicated with on an FM military network due to distances or a lack of system interoperability. Interestingly, the cell phone companies were able to restore roughly 97 percent of their network capacity within three weeks of Katrina's striking the coast. The problem was that calls were often blocked, because the network operated at 140 percent capacity during daylight or peak usage hours most days. The usage of the wireless network was so high because the land line system was virtually destroyed. Thus, almost all calls were hitting the wireless network. This was caused by severe damage to the land-line telephone system. Elevated phone lines had been blown down by surface winds in excess of 150 mph, and underground telephone switches were often flooded and ruined. This would take months to fully repair.

Even though most cell phone towers were damaged or destroyed, the network was quickly re-established through the use of devices like the Cell On Light Trucks (COLT). (See figure 4). COLTs are CDMA, GSM, and Satellite capable. They can carry both voice and data traffic and have similar band-width to many fixed cell tower assets. The difference is they are mobile, can be protected until a storm passes, and then rapidly deployed to bring cell coverage back on line.

Figure 4: Cell on Light Truck[20]

In addition to couriers, FM communications, and cell phones, my unit also used satellite phones, FRS/GMRS radios, and later, to a lesser extent, land lines as they came back into service. Satellite phones were the most reliable form of communication for "long haul" communications. Unfortunately, there were never enough of them to go around. They were generally restricted to battalion or brigade commanders and above on the military side. On the civil government and NGO side, satellite phones were more prevalent. Media outlets had the most satellite communications available by far. Media outlets also used up most of the available satellite bandwidth. FRS/GMRS radios were mainly used to link our 54 checkpoints to each other and back to the platoon and company command posts. These connections offered mutual support and allowed the guards on duty to report problems. While these radios were extremely reliable and easy to power with readily available AA batteries, they had limited range and no ability to carry data. However, they fulfilled the purpose of providing low-cost, reliable, short-range, albeit insecure, tactical communications.

We were able to get limited but reliable use of regular telephone land lines approximately 1 month after the storm hit. This was most useful for data communications, such as email. The limiting factor with dial-up data access is bandwidth, but slow email is better than no email.

In terms of data, the discussion of network links would be incomplete without noting the impact of commercial, wireless data connectivity. Even with the heavy use of the wireless network, we were able to get reliable data connectivity in low use hours (mainly

[20] Magnatek Website. Available online at <http://www.magnetektelecom.com/tpgproductsmobilecomm_colt.htm>.

late at night) using wireless broadband cards from Verizon and Cingular. We were able to email and share large files in non-peak usage hours very effectively. Instant Messaging also became available through this technology. Combining these cards with laptops allowed us to create a fairly reliable data network with surprisingly robust bandwidth. The effectiveness, ease of use, and cost of this solution made it very attractive during Operation *Vigilant Relief*. Figure 5 shows examples of some of these cards.

Figure 5: COTS Wireless Access Cards[21]

The good news is that TF Stonewall was able to develop a working voice and data network fairly rapidly with commercial off-the shelf (COTS) technology to reinforce the existing military communications suite. While these technologies often were not fully encrypted and secure, the nature of the mission made that an acceptable risk. Additionally, while the data network did not have great bandwidth, it was better than no data network. Satellite communication was by far the most flexible and resilient, but it was the least pervasive at the company, battalion, and brigade task force levels. Initially during the operation, Satellite communication also provided the best "reach-back" communication (communication with higher headquarters) outside the area of operations. In our case, that was reach-back communication to the Virginia JOC. Once terrestrial-based cell coverage was restored, reach-back communication became much easier and wide spread.

Summary and Lessons Learned

Operation *Vigilant Relief* taught us several lessons about how to prepare for and respond to complex humanitarian disasters, especially in terms of communication networks. The lessons learned can be grouped into four categories:

- Policy and Planning
- Technology and Equipment
- Training
- Unit Tactics, Techniques and Procedures

[21] Verizon Wireless Website. Available online at <http://www.verizonwireless.com/b2c/mobileoptions/broadband/serviceoverview.jsp>.

Policy and Planning Lessons

- The hardest part of developing an ad hoc network during a CHD is determining the nodes that exist in the network and keeping the network updated.
- Network centric operations are more than equipment, its people and processes.
- The "battlespace" we will occupy in a CHD domestic support operation will be larger than we expect making C^4I and information sharing much more difficult.
- The only network you can rely on is the one you bring with you. Units deploying to CHD environments must be as self supporting as possible and expect little to no re-supply in the first 96 hours.
- Deploy with spare parts for communication gear and other mission critical equipment.
- Adjacent Municipalities may differ greatly on policy issues that create confusion among the populace and degrade response effectiveness.
- The current military transformation does not transcend interagency boundaries. (Civilian agencies don't have Blue Force Tracker.)
- Military organizations and processes have the ability to rapidly bring order to interagency confusion. We train to cooperate and task organize in an ad hoc fashion.

Technology and Equipment

- Our current, organic communication equipment is inadequate for interagency communication.
- 802.11B/G and Bluetooth were not robust enough for our needs in terms of range
- 802.16E WIMAX may well be the low cost, commercial off the shelf solution for data connectivity in a CHD environment.
- Commercial laptops with wireless cards to access cell networks worked very well to get data communications up and running (satellite GSM cards were even better from a quality of service perspective)
- Guard units still lag far behind their active duty counterparts in fielded digital communication systems which degrades the Guard's effectiveness as well as a comprehensive common operating picture.

Training

- Developing a network under mission and time pressure in a CHD environment is hard and you need to train for it.
- Training for disaster relief and domestic support operations is very similar to training for Stability and Support Operations (SASO).
- SASO staff training using JANUS is an excellent training tool for improving staff effectiveness and vetting unit Standard Operating Procedures (SOPs) for disaster relief.
- Interagency training and rehearsal is absolutely fundamental to real disaster preparedness. We do not do enough of it.

- Train officers and senior NCOs in the fundamentals of continuity of operations.

Tactics, Techniques and Procedures

- We need to add a section to our battalion, company and platoon SOPs for supporting domestic civil authorities and non-governmental relief organizations.
- If possible, acquire first responder radios for the TOC and company command post. This will link the military net to the first responder net using a human interface (a radio telephone operator).
- Deploy with as many OE-254 long range antennae as possible.
- Deploy with as many generators as possible
- Deploy with a satellite phone assigned to all commanders.
- Assign a liaison officer to each municipal leadership team for communication, information sharing and relationship building.
- Where possible assign units to specific municipalities for ease of command and control and relationship building. As an example, I assigned Bravo Company to Biloxi, MS and Alpha Company to Long Beach.
- Battery use will be extremely high, bring lots of extras and use rechargeable batteries where possible.
- Begin immediate patrolling upon arriving in the area of operations to build a list of nodes for the network as quickly as possible.

This list of lessons learned is not comprehensive, but it highlights the key points. There is no doubt that those reviewing the case study will discover additional lessons learned.

In many ways, this operation was a dress rehearsal for an even bigger disaster of either natural or manmade origins. The scale and scope of Katrina had never before been experienced on U.S. soil. Moreover, the National Response Plan was effectively untested and unrehearsed for a disaster of this magnitude. One can expect that National Guard units like TF Stonewall will be heavily used in future scenarios, since disaster response is a core mission of the National Guard. However, to make the response effective, planners must revise response plans, ensure adequate equipment acquisition and interoperability among agencies, and ensure that response plans are well rehearsed through interagency exercises. Done properly, interagency networks can be established with rather low-cost COTS technology. All that said, one of the most significant observations of those on the ground was that network-centric operations is about far more than technology and equipment. It is about policies and procedures that not only allow, but set conditions for, interagency cooperation and network development in the shortest possible time and in the worst possible conditions. By learning the lessons of Hurricane Katrina, we ensure the next response will be far better and more effective.

Instructor's Guide for Transformation for Disaster Relief Case Study

Introduction

The Transformation for Disaster Relief case study details the problems and some possible solutions to developing a hastily formed network when much of the local infrastructure is damaged, destroyed, or otherwise unavailable. It is important to note that the case study focuses only at the battalion level, and on a National Guard battalion at that. Yet the lessons learned can be applied at the tactical, operational, and to an extent, policy levels. Based on class composition, this case study and the attendant class discussion may cause great tension. Katrina was both the finest and worst hour for many agencies and institutions. The instructor must be aware of the emotions of students, which may be high in discussing this, because many students may have worked for the agencies named. In point of fact, much improvement has already been made in preparing for future disasters of this magnitude. Yet much work remains. The purpose of this case study is to place students as close to the tactical (battalion) level as possible and allow them to develop solutions to the problems we faced on the ground along the Mississippi Gulf Coast. This will afford the nation better-trained decisionmakers in the future, as they will have the benefit of our experience.

Learning Objectives

At the completion of the case study, students should have the following knowledge:

- Understanding at the most basic level of what comprises a network in terms of links and nodes in network-centric operations.
- The composition of a network in terms of links and nodes in a disaster zone.
- Understanding of the basic facts making up the case study, such as the strategic background, AO, battalion task force mission, critical tasks, agencies and organizations involved, and the chain of command.
- Challenges faced in developing a multi-agency, hastily formed network.
- An introduction to the solutions used and the development of some of his/her own solutions based on their understanding of the situation. This will be accomplished through a small-group, practical exercise.
- An appreciation for the problems rooted in technology, as well as those problems rooted in policies, techniques, and procedures.

Instructor Themes

During the discussion generated by this case study, the instructor may wish to emphasize some or all of the following themes to assist in students' retention of knowledge.

Policy and Procedure vs. Technology. Often during this case study students will gravitate toward finding technical solutions to interoperability for interagency response. This is no

doubt important and should be discussed. However, the most intractable problems are those related to the policies and organizational roles and responsibilities that govern the response. With adequate funding and acquisition discipline, interoperable communications can be developed and deployed. However, creating uniform responses across municipal, state, and federal jurisdictions is much more difficult and often overlooked. In real terms, both areas must be addressed, not one or the other. The instructor should encourage the holistic approach to problem-solving.

Planning vs. Rehearsing. During the case study, most student questions will address planning. Very few students will voice the need for rehearsal. In fact, the national response plan had been updated a few months before Katrina struck, but the dissemination and interagency rehearsal of that plan was almost non-existent. The results were obvious. Students must internalize the importance of rehearsing complex plans if they wish to have a positive outcome during a CHD. On a similar note, some students will press the singular value of simulations. Simulation is good, but simulation is not a stand-alone method for training and rehearsal. The instructor may offer that scenario-driven, command post exercises work well and are not cost prohibitive.

Information Sharing vs. Information Pushing. One network-centric concept that students often miss is the sharing of information versus the pushing of information. This is where technology plays a vital role. The case study illustrates an often low-tech approach to netcentricity. Information is usually pushed between command and control nodes, but it was rarely shared in the NCO sense. This is because there was no technological infrastructure to facilitate real-time sharing at multiple echelons. The instructor may wish to encourage thought in how best to develop a network that shares information instead of predominantly pushing information.

Interesting Case Study Points

There are numerous interesting points brought out in the case study. Students will mention more than are shown here, but these are ideas to facilitate the discussion.

Common Operational Picture. The U.S. military has Blue Force Tracker (BFT), but other government agencies do not. Indeed, most National Guard units do not have BFT. Therefore, it is much more difficult (and manual) to create a common operating picture and keep it updated in real or near-real time.

Constant Network Change. Because numerous NGOs entered and exited the AO on any given day, the network nodes were changing. Further, because infrastructure was coming back on line, the network links were also changing.

Posse Comitatus. While not a specific NCO concept, this point can cause confusion, and students need to be clear. The National Guard is usually under the control of state governors. The National Guard, while in a state active duty status or a U.S. Code Title 32 status, may be used for domestic law enforcement. However, if the President of the United States federalizes the Guard under U.S. Code Title 10, the National Guard is in

the same legal status as the active duty military and may not be used for domestic law enforcement.

Inconsistent Policies and Coordination of Civil Government. Most municipalities initially were "islands unto themselves." This led to confusion and frustration because of differing policies on such things as access to beach areas and curfews. Further, the coordination between municipal and state officials was very loose initially.

Global War on Terror. Effects of the Global War on Terror included a lack of some equipment and fewer units available from both Mississippi and Louisiana. Students should understand that planners must deal with shortages due to other priorities. These conditions will no doubt recur.

Practical Exercise

The following practical exercise is designed for students in small groups. The instructor ideally should assign four students to a team. Each team will get one scenario. Based on what was learned in the case study, each team should develop answers to the questions below and present them to the class.

Scenario 1: "Dirty Bomb" is detonated in Washington, D.C. Reagan National Airport is rendered unusable.

Scenario 2: Massive earthquake strikes San Francisco destroying 40 percent of the city, including most port facilities.

Scenario 3: Tsunami strikes Oahu, effectively destroying all port facilities in Pearl Harbor. Death toll is estimated at more than 40,000.

Scenario 4: Avian Flu (H5N1) virus mutates to spread easily among humans. The virus reaches the United States, initially in upstate New York and Minnesota. Within three weeks, mid-west and northeast states are reporting more than 700,000 cases.

Group Questions

Question 1: Identify the challenges to creating a hastily formed network in this scenario.

Question 2: Discuss techniques for overcoming these challenges.

Question 3: Describe how these challenges are unique to the specific scenario.

Question 4: What special technological and policy planning considerations must be taken into account for this scenario?