REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
10-05-2007	FINAL	

4. TITLE AND SUBTITLE
Humanitarian Assistance and Disaster Relief Communications for the 21st Century.

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Major Charles Daly, USA

Paper Advisor (if Any): **Captain Stephanie Helm, USN**

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

Communication requirements for a humanitarian assistance / disaster relief operations (HADR) differ from a conventional combat operation - the military commander requires a more unclassified, information sharing architecture to effectively collaborate and coordinate with the civilian agencies and organizations involved in such an operation. The military response is often at the operational level but there can be strategic effects on U.S. prestige and credibility in a given region. All combatant commands must be ready to respond to a humanitarian crisis or natural disaster and to do so effectively must share information with civilian entities in the operating environment. This paper will analyze Operation Unified Assistance, the United States Pacific Command's response to the 2004 tsunami natural disaster, draw conclusion about the communications architecture from this analysis and discuss the lessons learned that apply to the operational commander when considering HADR communications and collaboration.

15. SUBJECT TERMS
Humanitarian Assistance, Disaster Relief, Unified Assistance, Communications, NGO, IGO, Tsunami

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Chairman, JMO Dept
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		23	19b. TELEPHONE NUMBER *(include area code)* 401-841-3556

Standard Form 298 (Rev. 8-98)

NAVAL WAR COLLEGE
Newport, R.I.

Humanitarian Assistance and Disaster Relief Communications for the 21st Century

by

Charles Daly

Major, United States Army

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____

10 May 2007

Abstract

Communication requirements for a humanitarian assistance / disaster relief operations (HADR) differ from a conventional combat operation - the military commander requires a more unclassified, information sharing architecture to effectively collaborate and coordinate with the civilian agencies and organizations involved in such an operation. The military response is often at the operational level but there can be strategic effects on U.S. prestige and credibility in a given region. All combatant commands must be ready to respond to a humanitarian crisis or natural disaster and to do so effectively must share information with civilian entities in the operating environment. This paper will analyze Operation Unified Assistance, the United States Pacific Command's response to the 2004 tsunami natural disaster, draw conclusion about the communications architecture from this analysis and discuss the lessons learned that apply to the operational commander when considering HADR communications and collaboration.

Table of Contents

INTRODUCTION

For the next century, the role of the U.S. military in humanitarian assistance and disaster response (HADR) missions will be a critical consideration for the U.S. Regional Combatant Commanders (RCCs). The global reach of the U.S. military, its ability to move supplies to austere locations, arrive with medical "first responders", and provide a communications network – to name just a few key capabilities – seem to foretell a significant military contribution to future HADR situations, domestically and internationally. Besides being the right force for the mission, there are moral as well as practical reasons why a RCC might place high importance on these missions: moral, for the relief of human suffering; practical, because the military's actions, predominantly the U.S. "face" of a relief effort, can be a powerful producer of international goodwill, even with countries holding a previously negative attitude towards the United States.

Certainly there are significant differences between HADR operations and combat operations. In planning combat operations, regional combatant commanders and their staffs might put emphasis on certain principles of joint operations such as security, mass, surprise, and unity of command, as an example. In considering HADR operations, however, the commander's emphasis on certain principles might change (and shift to other principles like legitimacy or restraint) or he may even chose to deemphasize certain principles in order to achieve the objective. For instance, when planning HADR operations a commander might chose to ignore typical operational security (OPSEC) principles to facilitate information sharing with non-governmental organizations (NGOs), intergovernmental organizations (IGOs), or other U.S. agencies and improve the legitimacy of the U.S. effort. He would likely stress unity of effort vice command to integrate into the civil response effort.

A simple change of emphasis on a set of the principles of war, though, can have a profound and concrete change on the doctrine, training, and material resources planned for and employed in an operation, in this case HADR. Consider just one small aspect of the total military response in an HADR scenario: the communications architecture. Are communications requirements different for HADR operations vice major combat operations? How does the communications architecture, normally based on the principle of OPSEC, establish unity of effort with the interagency organizations, civil authorities, IGOs and NGOs in such a situation? Clearly, communication requirements for a HADR mission differ from a conventional combat operation - the military commander requires a more unclassified, information sharing architecture to establish unity of effort and effectively collaborate and coordinate with the civilian agencies and organizations involved in such an operation.

One might be tempted to think, "It is just communications –right? Everyone has a cell phone and a hotmail account; it can not be that hard to work with the civil entities." In an unaffected area, this might be true, but HADR operations often occur in areas where some natural disaster – earthquake, volcano, flood, hurricane, etc., has occurred and destroyed the infrastructure. Even if in the unlikely event the civilian telecommunications capability was completely untouched, most military organizations operate on the Secret Internet Protocol Router Network (SIPRNET) vice the open, unclassified Internet that civil agencies use.

This paper will use an analysis of Operation Unified Assistance (OUA), the U.S. Pacific Command's (USPACOM) response to the 2004 Tsunami disaster in the Southwestern Pacific region, to aid in drawing conclusions on the HADR communications architecture and forming lessons learned for future military planning and execution of HADR operations.

OUA is only an illustrative example – not all HADR missions will be exactly the same but the major themes presented by this case will likely prevail.

ANALYSIS OF COMMUNICATIONS IN OPERATION UNIFIED ASSISTANCE

On Sunday, 26 December 2004, the world's most powerful earthquake in more than 40 years struck deep under the Indian Ocean off the Indonesian island of Sumatra triggering massive tsunamis that affected 11 countries (appendix, fig 1.). UN estimates put the death toll at 229,866 people lost, including 42,883 missing.[1] Besides the terrible cost in human life, the tsunami wiped out hundreds of miles of coastline, including the telecommunications infrastructure.

The military response was swift in order to alleviate the human suffering. By 29 December, USPACOM launched Operation Unified Assistance (OUA) and established the Joint Task Force (JTF) 536 HQ in Utapao, Thailand, later redesignated as Combined Support Force (CSF) 536, under the command of U.S. Marine Corps lieutenant general Robert Blackman. He would remark ten days later, "We are here to… mitigate human suffering…in doing so we hope…we can…improve our opportunities here in the region…."[2] His comments capture both the moral ("…mitigate human suffering…") and practical ("…improve our opportunities…in the region…") aspects of the operation's mission. CSF 536's formal mission statement (highlights added by author) is below.

> CSF-536, in **support of USAID/OFDA**, provides humanitarian assistance/ disaster relief support to the **governments of Sri Lanka, Thailand, Indonesia** and other affected nations in order to minimize loss of life and mitigate human suffering. On order, **transition U.S. Military HADR activities to designated agencies and/or Host Nations**, in order to facilitate continuity of relief and redeployment.[3]

By 12 February 2005 the mission was complete and PACOM disestablished CSF 356.The last U.S. force in the region, the USNS Mercy departed the region on March 16, 2005.

The background info above highlights some key aspects of OUA. It required a quick military response, integration into civilian efforts (as bolded in the mission statement for the CSF) and their command and control (C2) structure while still maintaining some sort of military C2 organization to command and control the armed forces involved. The challenge that LtGen Blackman had was achieving a unity of effort with the civilian "force" employed in the operation. As outlined below, he intentionally overlooked traditional OPSEC considerations that a commander would normally emphasize in major combat operation in order to effect this information sharing.

Military C2 in Operation Unified Assistance

On the military side, the C2 structure was fairly straight forward. CSF 536 had subordinate to it three Combined Support Groups (CSGs) that LtGen Blackman aligned geographically, as shown in figure 2 in the appendix. Integral to the operation was a Combined Coordination Cell (CCC), which served the role of a civil military operation center and was a coordinating point for other militaries that were not comfortable serving in the CSF construct as well as the UN, IGOs, and NGOs.

One might think that at least within the military C2 structure the communications architecture would work adequately as it would in any major operation – this, in fact, was not the case. USPACOM's designed its communication architecture to support a *combat* operation C2 structure, not an *HADR* C2 structure. LtGen Blackman chose the NIPRNET as his primary network, based on the mission statement above ("…in support of USAID/OFDA…") but meanwhile not all elements of his force could operate easily on this

unclassified network. One example was the U.S. Navy -of the 15,490 U.S. personnel assigned to the CSF, 8,617 were from the navy with most of them assigned to the Abraham Lincoln Carrier Strike Group (CSG) or the Expeditionary Strike Group 5 (ESG-5).[4] The U.S. Navy, understandably so for OPSEC reasons, is used to working on the SIPRNET and did not configure both the CSG and the ESG with enough bandwidth for unclassified Internet. One navy captain remarked how difficult it was to go from a ship trying to be stealthy to one trying to transmit as much as possible.[5] The solution to this problem was to outfit CSF 536 with SIPRNET, but that did not occur until 7 January 2005 and even then, there were not many SIPR computers so the action officers at the CSF did not readily use them. Besides, the SIPRNET was not what any of the civilian agencies were using; it seems like the military was adapting the situation to their frame by increasing SIPRNET rather than the reality of working with civilian organizations by increasing NIPRNET.[6] A similar issue arose with the USPACOM staff. The USPACOM JOC was "living" on SIPRNET for the first few weeks of OUA and even after LtGen Blackman identified NIPRNET as the operational network, there were not enough NIPR terminals in the JOC.[7]

When looking at the military communication units supporting this C2 structure it is more notable to consider who was missing rather than who deployed in support of OUA. The Marines deployed the 9th Communications Battalion and the 7th Communications Battalion for the operation, while the Army sent the 56th Signal Battalion, but missing was the Joint Communications Support Element (JCSE). JSCE, a brigade sized communication element under the Joint Forces Command has the mission of supporting JTFs (or CSFs, in this case) and unified commands for both contingency and crisis operations.[8] The USPACOM J6 did not request JCSE until C+12 and they would not have even arrived until

C+20 due to deployment phasing. The CSF 536 J6 cancelled the requirement since he needed them earlier vice later in OUA.[9] JCSE has the institutional knowledge that spans all the regional combatant commands and is a repository for JTF level communications know how.

While the nature of OUA presented some issues for deploying the right communications architecture to support the C2 structure and the mission statement, the civil military relationship in OUA also produced some challenges.

Civilian C2 in 2004-2005 Tsunami Relief

As noted in the CSF 536 mission statement, the military was in support of the USAID/OFDA effort. In turn, all combined U.S. efforts were in support of the UN, the lead agency in the relief operations.

USAID was not set up to act as a supported military command; it did not have the organizational staff or the communications systems to conduct the normal interface one would see in a military organization. Also as a Department of State organization, they tended to align themselves more with each ambassador and his or her country team rather than work regionally, as the military did.[10] Both of these points have implications for the communications architecture used for effective coordination and collaboration (discussed in the Analytical Conclusion Section below).

Similarly, the UN did not command and control its operations in a traditional military sense. Figure 3 in the appendix is LtGen Blackman's impression of what the actual UN C2 chart was during the relief operations. As opposed to a traditional C2 chart, this one has many dotted lines and unclear relationships. The UN operates as a loose confederation of agencies and different NGOs are associated with the different UN agencies. It also is very ad

hoc and relies on constant crisis action procedures vice any contingency planning.[11] It does not deploy with much in the way of communications; it relies heavily on unclassified email and cell phones to communicate.

In both the case of USAID and the UN, as well as for all the other NGOs, IGOs, and host nation governments that were responding to the tsunami crisis, the key to military and civil integration was CSF 536's Combined Coordination Center (CCC) collocated in Utapao Thailand with the CSF HQ. Eleven foreign militaries were present at the CSF. There were also representatives from various UN agencies and the U.S. Country Teams from the affected areas.[12] What is notable however, is who was not represented – there were 22 other foreign militaries not in the CCC. Also not all the numerous NGOs and IGOs had LNOs; there were 68 NGOs operating in Indonesia and 84 operating in Sri Lanka, as an example.[13] The reasons might be due to a reluctance to work with the United States or it just might have been impractical for some aid organizations to send a liaison due to money or manpower. So, although the CCC was the hub of coordination, and it certainly contributed significantly to the unity of effort in OUA, what other tools and methods did the CSF have to coordinate and collaborate with the organizations that could not (or chose not to) have a physical presence in the CCC? This thought leads to the next (and last part) of the analysis of OUA – the use of virtual and collaborative tools during OUA.

Operation Unified Assistance Collaborative Tools

On the military side, there was some breakdown on the use of collaborative tools due to the emphasis on a more unclassified operating environment. For instance, U.S. Navy ships were used to using Internet Relay Chat (IRC) for ship to ship communications on SIPRNET but they did not have the same capability on the NIPR side and CSF 536 did not have IRC

capability on *either* NIPR or SIPR.[14] Meanwhile USPACOM staff used InfoWorkSpace (IWS) on SIPR.[15] Some of the other collaborative software used in CSF 356 were Asynchrony, Vogue, and Webex, all which had their own compatibility problems with each other.[16]

There were also problems created by working in a coalition environment especially since some foreign militaries responding to the crisis were not traditional partners of the U.S. For instance, although both Japan and Australia had Collaborative Enterprise Regional Information Exchange System (CENTRIXS) terminals meant specifically for a coalition environment involving the U.S., most of the other military participants, even those working directly with the CSF did not have those terminals.[17]

For the military to civilian coordination, one of the main tools used in OUA was the Asia-Pacific Area Network (APAN).[18] APAN is an unclassified web site hosted by USPACOM promoting security cooperation and collaboration in the Asia-Pacific area. The site still has an archived link to OUA and CSF 536 used it as the primary web based means to share and disseminate info to all the civilian agencies and organizations. APAN received mixed reviews. A USPACOM J723 briefing (note: the USPACOM J723 is the JTF Certification Branch) stated that it "…greatly increased the effectiveness of Combined Support Force and Combined Coordination Center Operations."[19] Other users were not as enthralled with the application. [20] According to the USPACOM J6 after action report, some DOD personnel had trouble accessing APAN. Civilians also had problems reaching the site partly due to the ".mil" domain issue that occurs on NIPRNET. Also, USPACOM cut funding for APAN before the tsunami, limiting its effectiveness.[21] Although in theory,

APAN seems like a valuable tool in an HADR scenario, in the reality of OUA this was not always the case.

At this point, one may be tempted to remark, "Ok, it seems like we need a more unclassified architecture for HADR communications – but what about OPSEC? Isn't that a basic tenet of ***any*** military operation?" Also, the open Internet is rife with hackers and organized, state sponsored elements attempting to "crack" U.S. Military networks. Although a valid point and OPSEC is indeed important in any scenario, OPSEC relates primarily to the enemy and the objective. This argument also emphasizes the major point of this paper – HADR communications are ***different*** than for a major combat operation. In a major combat operation, a commander employs OPSEC to keep information from the enemy and to safeguard the U.S. operations ideally directed towards a command objective. In an HADR scenario, human suffering is the enemy – there is no need to keep information from this foe. Instead, as the diverse agencies and military units cooperate in order to achieve their common objective (alleviate human suffering), information must be shared to maintain unity of effort. This scenario calls for all entities to resort to the lowest common denominator for security – the open Internet – to enable coordination. This does not mean that J6's connect SIPRNET to the NIPRNET, for example; RCCs must still ensure that the proper firewalls and network security procedures are in place. A future enemy might use a HADR operation as an opportunity to exploit the military's network.

CONCLUSIONS DRAWN FROM OPERATIONS UNIFIED ASSISTANCE

There are some main conclusions drawn from an analysis of OUA. They are presented below to flow from one conclusion to the next in a logical manner- one conclusion

naturally leads to the next as they span from a broad perspective on the OUA network, to the unique nature of OUA and its implication for the network planning and execution, to conclusions about specific segments of the network – military and civilian.

OUA: Requirement for a More Open Internet Communications Architecture

As in most HADR operations, the U.S. Military was not the lead agency; in this case, the USAID was the supported entity. USAID, in turn was supporting the UN efforts to mitigate suffering in the region. Subsequently, OUA required the CSF to conduct a significant amount of coordination with host nation governments, the UN, NGOs, IGOs, and foreign militaries the U.S. did not normally communicate with (Indonesia, for one). There was no common network available to all to coordinate and collaborate to achieve the same objective. Even the NIPRNET is not sufficient – the NIPRNET is a ".mil" domain on the Internet that can restrict viewers to web pages if they are not U.S. military (as mentioned above in the APAN discussion). OUA required a truly open Internet architecture to span all the organizations involved.

OUA: Quick Response and Short Timeline

Planning time was truly abbreviated when compared to other crisis action "combat" events, for instance the U.S. reaction to Iraq's invasion of Kuwait. Also, the timeline of the operation was relatively short, about one month. When the USPACOM J6 attempted to get JSCE into the operation (as mentioned above), they were too late into the operation (since it was ending in a few weeks) and the idea was abandoned. For typical combat operations, this request would have been early in the process, even for crisis action planning. In this case though, "mass" and building up forces were not the consideration, saving lives quickly was.

U.S. Military: Not Used to Working on the Open Internet

One could even say the military is not used to working on NIPR, let alone the open Internet.[22] One of the tenets of Net Centric Warfare is a seamless extension of the garrison network to the deployed operations – effectively there is only one network, not one that is "deployed" vice used in garrison. Net Centric warfare did not work in OUA – USPACOM would not normally "fight" off NIPR or the Internet and they certainly would not extend either downrange to such a large scale as required in OUA. This was obvious in OUA when one considers the U.S. Navy's and USPACOM's JOC use of predominately SIPR. Even though the CSF 536 commander (rightly so) designated the Internet as his operational net, different components of his force were not ready to operate this way, including his higher HQ. Part of this is equipment and employment – even if the Navy wanted to get on NIPR, they did not have the bandwidth allocated (besides for morale purposes) to it and the ability to reconfigure their bandwidth from SIPR to NIPR on the fly.[23] There was also a mindset issue - this is evident that the fix to the connectivity issue between the U.S. Navy, the USPACOM JOC, and CSF-536 was to increase the amount of SIPR at the CSF HQ rather than get USPACOM and the Navy on NIPR. One account of the U.S. Navy's use of unclassified Internet in OUA recalls "… most of the flag staff members were using unclassified email accounts, which were not safe from an operational security perspective."[24] What does "not safe" mean? And not safe from what? Is OPSEC really a concern here? A user only needs to provide vague and, if they chose, inaccurate information to set up a hotmail account, for instance. Secondly, the info they are sending, conceivably about the coordination of aid with an NGO, contains limited security information.

The U.S. Military had Collaborative Tool compatibility Issues

Even, if the U.S. was used to working on the open Internet or when they used SIPRNET in OUA, they still have problems with collaborative tool capability. The different collaborative tool suites that were referenced above can best sum this up: IWS, Webex, IRC, Asynchrony, and Vogue, not to mention the Defense Collaborative Tool Suite (DCTS). Used effectively, these tools go beyond simple email – they allow real time "virtual" meetings, virtual "whiteboard" sessions, chat sessions, to name a few of the capabilities. Instead of point to point communications (email) these tools allow point to many information sharing (i.e., a web posting). There was no standardization of the software suites across the CSF (or USPACOM), however, on any network during OUA.

The Civilian and Foreign Military Collaborative Environment – More Complicated than the Military Environment

This might also be termed "Even if the military figured out their collaborative tool problem, it would not solve the bigger collaboration problems." As a generalization, the civilian organizations involved in the tsunami relief effort used more ad hoc arrangements and were loosely organized (as the UN Chart displays in fig. 3). Open Internet was not enough in OUA, even when available – there was a needed collaborative environment to coordinate with civilian entities as well as other militaries. It would be unreasonable to expect all the civilian and foreign military elements to have arrived to the relief activities with a common collaborative tool suite – the software changes too fast, some elements could not afford the software, and some organizations would not normally cooperate willingly with the U.S. military outside of the relief operations. The CCC attempted to provide a collaboration environment in a ***physical*** way, but not all NGOs, IGOs or foreign militaries participated.

APAN was the effort to set up a ***virtual*** coordination and collaboration environment, but as mentioned in the analysis it had some funding problems and usability issues for both the military and civilian elements involved in the relief effort. Conceptually, though, the APAN was the best attempt in this case to enable this virtual information sharing- it does not rely on any compatibility standard as long as a person could get on the Internet and get to the web site (which was not always the case, unfortunately). It operated more as a post office box vice a mailbox – users had to "travel" to the PO box (website) to check the information rather vice the post office delivering their "mail" directly to them (email or chat).

LESSONS LEARNED

The paper so far has examined OUA by analyzing the operation and drawing conclusions to demonstrate that communication requirements for a HADR mission differ from a conventional combat operation – there is a greater need for a more unclassified, information sharing architecture to establish unity of effort and effectively collaborate and coordinate with the civilian agencies and organizations involved in such an operation. The lessons learned in this section are more generic in nature (although they certainly apply to OUA) and have applicability across all the Regional Combatant Commands. Once again, no two HADR mission will be exactly alike and OUA was only an illustrative example but aspects of OUA provide lessons that will likely apply in most HR/DA missions. The lessons below correspond directly with the conclusions noted from above.

Open Internet Communications Architecture through Equipment, Training, and Doctrine (from conclusion A and C).

The following is an excerpt from the U.S. Joint Publication on Foreign Humanitarian Assistance and Planning (bolded words appear as in the publication): "**Direct**

communications between commanders and nonmilitary organizations should be established to facilitate effective coordination and decision making."[25] But how does a RCC actually go about doing this? There is a lot implied in that statement for the equipping, training and the policies for operating a JTF level HQ in support of a HADR mission.

Equipment is the first leg of establishing a viable, open Internet architecture as RCCs prepare for HADR missions. One solution to equipping individual users with "Internet" ready computers is to buy a separate set of hard drives for open internet use – after a HADR operation is complete, commands can be electronically wipe and store them for future missions. Also, the RCC HQs should have sufficient internet drops in their JOC or applicable operations center. The J6 does not need to have these drops activated all the time and actually they could lie dormant normally until needed for HADR or other operations. On the network side, it is less challenging – J6's regularly provide NIPRNET in the operational communications architecture, just not to the bandwidth needed for an HADR operation. This is a matter of configuring the architecture so J6s can allocate the bandwidth as needed.

Training is the second leg of the supporting the use of the Internet - RCC s must actually use the open internet and associated tools and websites during their operational exercises preparing for HADR response. This is the time to reinforce the unclassified Internet as the most likely "network of choice" for the operational commander during HADR operations and these training scenarios should generate the analysis and thought on what that particular command requires to employ it. Training during these exercises should also strive to counter the natural tendency of most well-intentioned, OPSEC minded, service members as long as RCCs develop the proper policy for unclassified Internet use, which leads to the third aspect, policy.

Rather than have each unified command determine their policy for internet use for HADR operations, it should doctrine from the U.S. Joint level. Although the Joint Publication on foreign HA implies Internet use, it should be more doctrinally specific (perhaps by using the word "Internet") on the nature of the HA communications. Also the Defense Information Systems Agency (DISA) has a policy role setting the boundaries for Internet use and what are the proper security procedures that will allow for free sharing of information while protecting military information.

Contingency Planning for a Crisis Action (from conclusion B)

Although natural disasters require a quick response, general contingency planning for them should be an ongoing activity within a RCC. Some of the planning considerations for a HADR contingency plan are scalability (to cover a small to large response), collaborative tools available to all, including civilians, and forces involved. When the HADR crisis does occur, the J6 can adapt the plan quickly to meet the developing situation.

JCSE is a key to this quick response – they are the subject matter experts on JTF communications, and are configured for quick response when needed. The RCC J6 should plan for them in the HADR contingency plan and then ask for them upfront in a crisis. Even if it is a relatively small HADR response, JCSE has small planning teams that can augment the J6 and lend their centralized knowledge to the effort. Specifically to HADR operations, they must develop the ability to extend the unclassified Internet using their communications network.

Military Collaborative Tools – Set a Standard (from conclusion D)

There is currently no approved collaboration tool across all the services that span the unclassified networks and SIPRNET. The Joint Chiefs of Staff (through Joint Forces

Command) should designate what the collaborations tool is. It does not matter what it is specifically, as long as it is the same across the NIPRNET and SIPRNET so that personnel do not have to train on multiple software tools. Also, it should work in low bandwidth environments and be a commercial off the shelf application so civil elements can use it to collaborate during HADR operations if they chose. This particular lesson learned is not just applicable in HADR operations but in most of the range of military operations. As displayed in OUA, there is a wide variety of collaboration tools on all the networks a RCC deploys.

The Civ- Mil Collaborative Environment – Central Management (from conclusion E.)

APAN in concept was a decent solution to setting up a virtual collaborative environment for USPACOM, but is it applicable across all the RCCs? For instance, say the UN had to respond to a natural disaster in the USEUCOM area of responsibility. Would they be expecting the same coordination website they saw in USPACOM? Across the RCCs, there are likely several different "APANs" with a different appearance and mode of use. In a HADR response, however, many of the civil organizations responding to the crisis, like the U.N. and USAID, are not regionally aligned. In other words, the same folks that showed up for the Tsunami relief might be the same people that show up for the next HADR response in USEUCOM. This holds true for some of the NGOs as well.

The United States Joint Forces Command (USJFCOM) should be the central manager of a HADR collaborative website- from that site each of the RCCs can have a link to their particular site, but it should look and "feel" the same as USJFCOM's site. This will condition all the international elements that typically participate in HADR responses to automatically go to that site when coordinating with the U.S. military. An added benefit to this is JCSE is a sub-unified command under USJFCOM. USJFCOM will own both the

communications architecture and collaborative tools to respond to HADR missions. There is no one specific web style that is needed, as long as non ".mil" addresses can access it, it is fairly easy to use and understand, and USJFCOM sets up a registration process that is responsive to the changing nature of the civilian response to HADR scenarios. In other words, organizations can pre-register so they are ready to work with the military immediately during a HADR scenario. It is also important that commands constantly man the site with support and keep it active to respond quickly to crisis (warm start vice cold start).

FINAL REMARKS

Plainly, the U.S. military has the resources to respond to an HADR scenario; however, there are different principles of joint operations applied to these operations when compared to combat operations. In a HADR operating environment, a JTF commander will put more emphasis on information sharing and unity of effort with his or her civilian counterparts and less emphasis on information security. As a consequence, the communication requirements for a HADR mission differ from a conventional combat operation - the military commander requires a more unclassified, information sharing architecture to establish unity of effort and effectively collaborate and coordinate with the civilian agencies and organizations involved in such an operation. There are steps the RCC can take (with the help of USJFCOM) to better equip, plan, and prepare his command for the next natural disaster or humanitarian catastrophe.

ENDNOTES

1. United Nations, Office of the Special Envoy for Tsunami Recovery, "The Human Toll," 2006, http://www.tsunamispecialenvoy.org/country/humantoll.asp (accessed 03 April 2007).

2. Al Pessin, "US Commander Says Peak of Tsunami Crisis Near, Focus Shifting to Long-Term Needs", Voice of America, 7 January 2005, http://www.globalsecurity.org/military/library/news/2005/01/mil-050107-237c3543.htm, (accessed 04 April 2007).

3. Robert Blackman, Jr., "Observations on HADR Operations," PowerPoint, 25 Jan 2006, Quantico, Virginia: CAPSTONE Briefing.

4 . United States Navy Warfare Development Command, "NWDC Tsunami Lessons Learned," 2005, http://www.nwdc.navy.smil/nlls/nllweb/search/hadr.aspx (accessed 27April 2007).

5. Bruce A. Elleman, *Waves of Hope: The U.S. Navy's Response to the Tsunami in Northern Indonesia*, Newport Paper 28 (Naval Station Newport, RI: Center for Naval Warfare Studies, Naval War College, February 2007), 71.

6. Ibid., 72.

7. United States Pacific Command J6, "Operation Unified Assistance J6 Lessons Learned," February 2005, http://www3.gsf.hq.pacom.smil.mil/J7web/J72/J723/index.aspx?ct=6&cp=8 (accessed 27 April 2007), III.A.1-2.

8. Joint Communications Support Element, "Mission," http://www.jcse.mil/our_mission.htm (accessed 09 May 2007).

9. United States Pacific Command J6, "Operation Unified Assistance J6," I.C.1.

10. Blackman, "Observations on HADR Operations."

11. Ibid.

12. Ibid.

13. United States Pacific Command, "Operation Unified Assistance Lessons Learned," PowerPoint, 07 June 2005, http://www3.gsf.hq.pacom.smil.mil/J7web/J72/J723/index.aspx?ct=6&cp=8 (accessed 09 May 2007).

14. Elleman, *"Waves of Hope,"* 72.

15. United States Pacific Command J6, "Operation Unified Assistance J6," III.A.6.

16. Elleman, *"Waves of Hope,"* 76.

17. Ibid, 73.

18. APAN can be accessed at this web page: http://www1.apan-info.net/.

19. United States Pacific Command J723, "J723 Operation Unified Assistance Lessons Learned, Rev 4," PowerPoint, 25 Mar 2005, http://www3.gsf.hq.pacom.smil.mil/J7web/J72/J723/index.aspx?ct=6&cp=8 (accessed 27 April 2007).

20. United States Pacific Command, "Observations on Unified Assistance", 23 February 2005, http://ww2.hq.pacom.smil.mil/common/lessons (accessed 09 May 2007).

21. United States Pacific Command J6, "Operation Unified Assistance J6," III.C.2.

22. Author's Note: Once again, the open Internet is *different* form the NIPRNET. Any ".mil" web site or email address resides on the NIPRNET, which is protected by DOD from the INTERNET. This protection can cause access problems for non-DOD Internet users as they attempt to collaborate with the military.

23. Elleman, *"Waves of Hope,"* 73.

24. Ibid, 72.

25. Chairman, U.S. Joint Chiefs of Staff, Joint Tactics, Techniques, and Procedures for Foreign Humanitarian Assistance, Joint Publication (JP) 3-07-6 (Washington, DC: CJCS, 15 August 2001), IV-9.

Appendix (Figures)

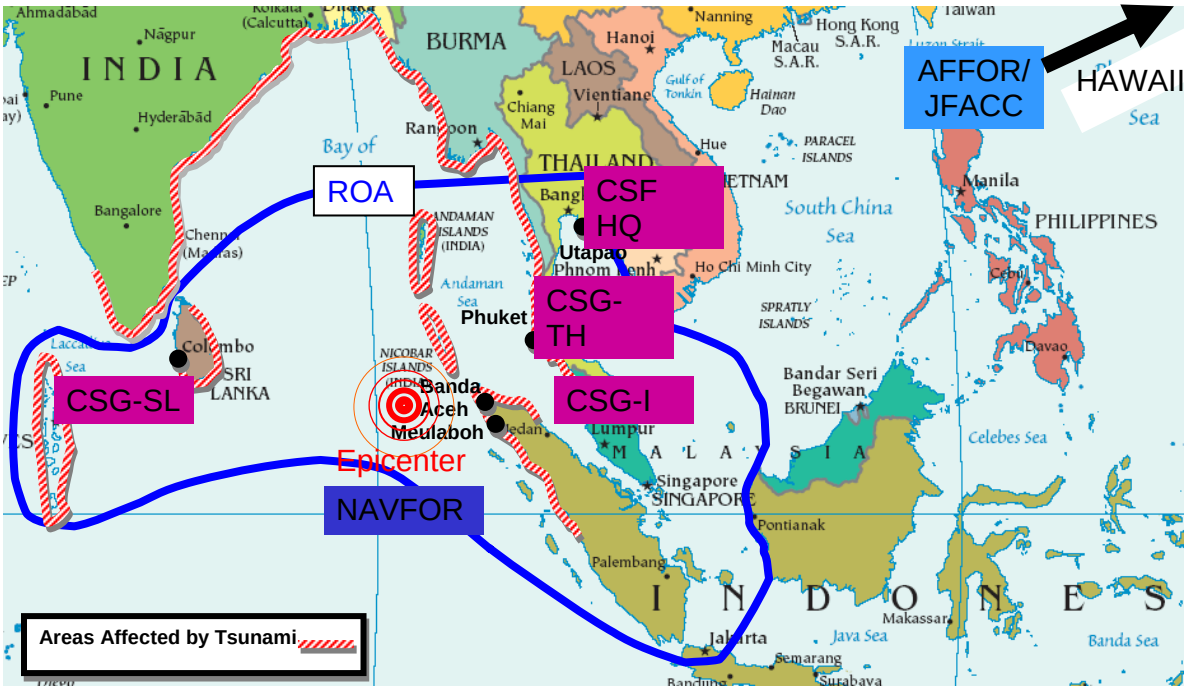

Figure 1. Areas Effected by the Tsunami, with military area of operations added (reprinted from Robert Blackman, Jr., "Observations on HADR Operations," PowerPoint, 25 Jan 2006, Quantico, Virginia: CAPSTONE Briefing).

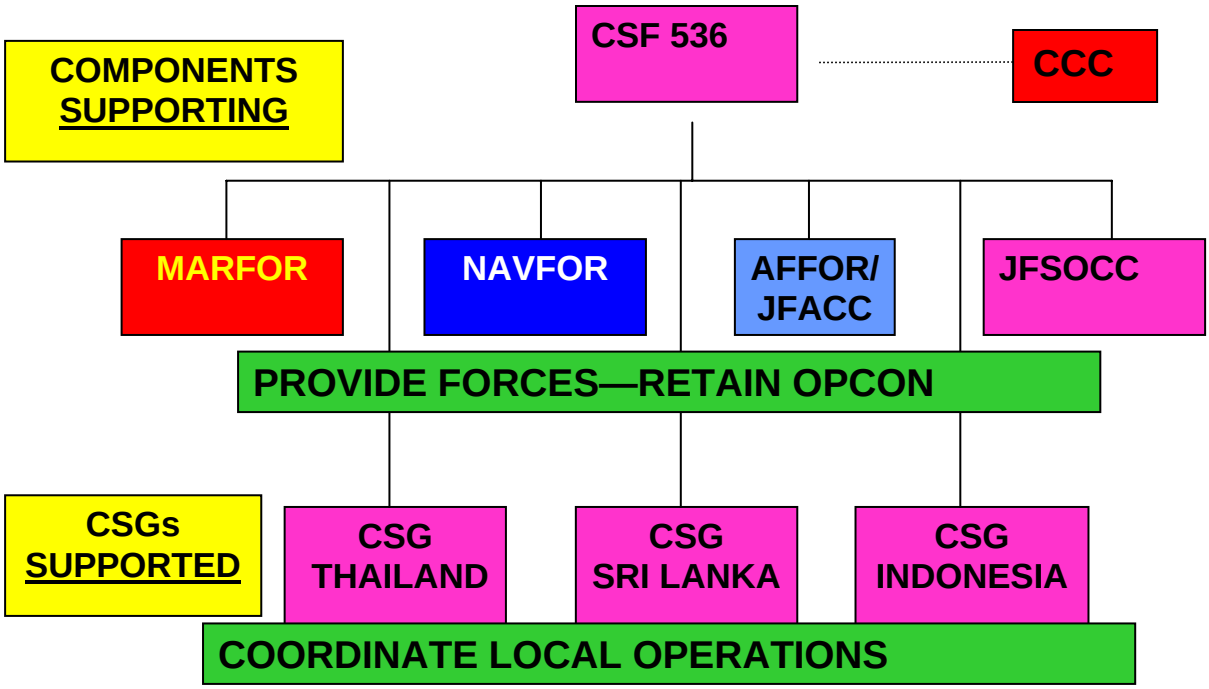

Figure 2. CSF 536 C2 Structure for OUA (reprinted from Robert Blackman, Jr., "Observations on HADR Operations," PowerPoint, 25 Jan 2006, Quantico, Virginia: CAPSTONE Briefing).

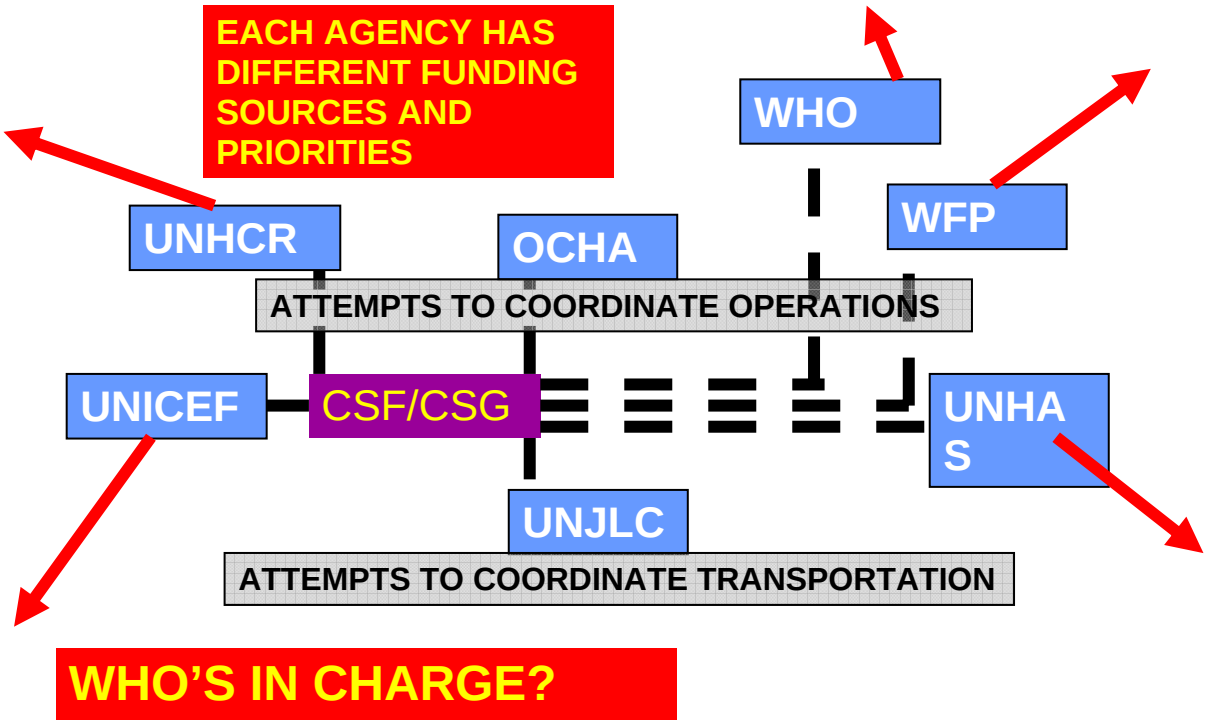

Figure 3. UN C2 Structure for OUA, as perceived by LtGen Blackman, CSF 536 Commander (reprinted from Robert Blackman, Jr., "Observations on HADR Operations," PowerPoint, 25 Jan 2006, Quantico, Virginia: CAPSTONE Briefing).

BIBLIOGRAPHY

Blackman, Robert Jr. "Observations on HADR Operations." PowerPoint, 25 Jan 2006.

Daniel, James. "Operations Unified Assistance: Tsunami Transitions." Military Review 86, no. 1 (January / February 2006): 50.

Dorsett, David. "Tsunami! Information Sharing in the Wake of Destruction". Joint Forces Quarterly, no. 39 (4th Quarter 2005): 12-18.

Elleman, Bruce A. *Waves of Hope: The U.S. Navy's Response to the Tsunami in Northern Indonesia*, Newport Paper 28. Newport, RI: Center for Naval Warfare Studies, Naval War College, 2007.

Joint Communications Support Element's Official Web Site. http://www.jcse.mil/our_mission.htm (accessed 09 May 2007).

Pessin, Al. "US Commander Says Peak of Tsunami Crisis Near, Focus Shifting to Long-Term Needs." *Voice of America*, 7 January 2005. http://www.globalsecurity.org/military/library/news/2005/01/mil-050107-237c3543.htm, (accessed 04 April 2007).

United Nations. *Post-Tsunami Lessons Learned and Best Practices Workshop: Report and Working Groups Output*. United Nations Report. Jakarta, Indonesia: United Nations, May 2005.

United Nations, Office of the Special Envoy for Tsunami Recovery. "The Human Toll." http://www.tsunamispecialenvoy.org/country/humantoll.asp (accessed 03 April 2007).

U.S. Congress. Senate. *Tsunami Response: Lessons Learned: Hearing before the Committee on Foreign Relations.* 109th Cong., 1st sess., 2005.

U.S. Department of Defense Technical Information Center. "The Worldwide Lessons Learned Conference 2005: Case Study: Operations Unified Assistance." Joint Electronic Library. http://www.dtic.mil/doctrine/wjllconference05.htm (accessed 9 May 2007).

U.S. Office of the Chairman of Joint Chiefs of Staff. Joint Tactics, Techniques, and Procedures for Foreign Humanitarian Assistance. Joint Publication (JP) 3-07-6. Washington, DC: CJCS, 15 August 2001.

U.S. Navy. “NWDC Tsunami Lessons Learned.” United States Navy Warfare Development Command. http://www.nwdc.navy.smil/nlls/nllweb/search/hadr.aspx (accessed 27April 2007).

U.S. Navy. Office of the Chief of Naval Operations. "Humanitarian Assistance/Disaster Relief (HA/DR) Operations Planning.” TACMEMO 3-07.6-05. Newport, RI: Navy Warfare Development Command, August 2005.

United States Pacific Command. “Observations on Unified Assistance”, http://ww2.hq.pacom.smil.mil/common/lessons (accessed 09 May 2007).

United States Pacific Command. “Operation Unified Assistance Lessons Learned.” PowerPoint, 07 June 2005.

United States Pacific Command. *Operation Unified Assistance Tsunami Relief: Online Archive*. http://www.pacom.mil/special/0412asia/ (accessed 9 May 2007).

United States Pacific Command J6. “Operation Unified Assistance J6 Lessons Learned.” http://www3.gsf.hq.pacom.smil.mil/J7web/J72/J723/index.aspx?ct=6&c=8 (accessed 27 April 2007).

United States Pacific Command J723. “J723 Operation Unified Assistance Lessons Learned, Rev 4.” PowerPoint, 25 Mar 2005.