Perspectives on Information and Communications Technology (ICT) for Civil-Military Coordination in Crisis

Gerard Christman

Office of the Assistant Secretary of Defense for
Networks and Information Integration (OASD(NII)),
Directorate for Contingency Support and Migration Planning (CSMP)

Franklin Kramer, Stuart Starr, Larry Wentz
National Defense University (NDU), Center for Technology and
National Security Policy (CTNSP)
2006 CCRTS

Slide 1
This presentation was derived from the development of a Primer that describes Information and Communications Technology to support Civil-Military coordination during Humanitarian Assistance / Disaster Relief (HADR) and Security Stability Transition and Reconstruction (SSTR) Operations. The Primer stemmed from input derived from numerous workshops and interaction involving civilian and military practitioners from inside and outside the US Government.

The impetus for the Primer stemmed from perceptions that recent US HADR and SSTR operations needed to be improved. In addition, perceptions were also that lessons learned and current observations from practitioners needed to be fedback into the various processes to modify training education, doctrine, and policy.

As stated on the title slide, both the Center for Technology and National Security Policy and the Office of the Assistant Secretary of Defense for Networks and Information Integration working in partnership to conduct the workshops and solicit the information that provided the baseline from which to develop the Primer.

Slide 2
The agenda helps you understand how I've structured the presentation. It tracks well with the Primer and the associated paper presented at the Command and Control Research and Technology Symposium in June 2006.

Slide 3
There are several types of crisis operations. HADR operations are short duration, expeditionary operations focused on saving lives and assisting in mitigating the effects of disasters. Whereas SSTR operations are generally longer term operations focused on major reconstruction projects. In both types of operations, numerous entities including the military respond. In order to harness the capabilities of these numerous respondents a collaborative environment needs to be established. If the collaborative environment is

not established, the respondents may be working aspects of the operation that may become redundant, counterproductive, or dangerous. We seek to create an environment where information that all respondents seek may be found. The DoD may have information or products that others seek. Similarly others may have knowledge or information that the US seeks. Again the goal is to leverage every bit of capability of all entities that arrive on the scene to deal with the operations. The sooner this is done, the sooner the military can be redeployed, refit, and readied for another fight.

Slide 4
The key here is that regardless of the type of crisis, there are many similarities with regard to Information and Communications Technology used in reaction to them. It is vital that we understand what we expect to have to deal with during these operations so we can plan accordingly.

Slide 5
This slide simply speaks to the Primer and the way we've organized.

Slide 6
Each responder needs information in order to fulfill their responsibility. The challenge is that every responder arrives with differing ICT where some are more capable than others. There is seldom the luxury of time to sort through these capabilities and limitations to develop a cross referenced matrix. However, the landscape is not all bleak. There are some common capabilities that seem to arrive fairly consistently. Again, the key is to seize upon them and plan accordingly.

There is also sensitivity to dealing with the US military. There is a suspicion that the US military may be intelligence gathering as well. One must be cognizant of this and if one is part of the US military establishment, try to be sensitive to this and allay these suspicions. Indeed sharing US military capacity with other responders can go a long way to building trust and partnership.

As always there are cultural considerations in these types of operations too. Military culture and local culture may not be in synch. Gender roles, body language, spoken language, language proficiency, and others aspects of culture and communications all come into play. There are similarities in cyber space too. For example communications in all capital letters is considered shouting and rude. Emoticons included in mail may seem unprofessional to some. Domain specific jargon and acronyms can become problematic as well as more time is consumed explaining things than is given to relief efforts.

Slide 7
This concludes part 1 of this presentation. Part 2 is located in the Network Architecture in this site. The full primer is located under the Resources area of this site. Close this browser window to exit.