Information Communications Technology (ICT) Support to Complex Emergencies

Larry Wentz

Stuart Starr, Ph.D.

Center for Technology and National Security Policy
National Defense University
Fort McNair, Washington, D.C., U.S.A.
e-mails: wentzl@ndu.edu
starrs@ndu.edu

Larry Wentz is a Senior Research Fellow at the National Defense University Center for Technology and National Security Policy. Prior to joining NDU, he was a Research Scientist at the George Mason University (GMU) Center of Excellence in C3I. And prior to this assignment, he was the director of the ASD (C3I) Command and Control Research Program (CCRP) sponsored lessons from Kosovo study in 1999-2001 and held a similar CCRP position in 1996-1998 when he was on a special government assignment from the MITRE Corp to the National Defense University (NDU) and conducted the lessons from Bosnia study. Mr. Wentz completed 30 years with the MITRE Corp of which 18 were spent on assignment at NATO Headquarters. He is a writer, author, and lecturer on multinational C4ISR systems interoperability, multinational civil-military collaboration and information sharing, Information Operations and Civil-Military Operations.

Dr. Stuart Starr is a Distinguished Research Fellow at the Center for Technology and National Security Policy, National Defense University. Concurrently, he serves as President, Barcroft Research Institute (BRI), where he consults on Command and Control (C2) issues, serves on senior advisory boards to defense industry (e.g., Northrop Grumman, Titan), lectures to audiences world-wide on C2 issues, and participates on Blue Ribbon panels (e.g., member of the Army Science Board (ASB); member of the National Research Council Task Force on Modeling and Simulation (M&S) to support the Transformation of DoD). Prior to founding BRI, Dr. Starr was Director of Plans, The MITRE Corporation; Assistant Vice President for C3I Systems, M/A-COM Government Systems; Director of Long Range Planning and Systems Evaluation, OASD(C3I), OSD; and Senior Project Leader, Institute for Defense Analyses (IDA).

INTRODUCTION

The components of civil-military coordination consist of information sharing, task sharing and joint planning. The challenges include issues such as intelligence versus information, military classification versus civilian need for transparency, command and control of military versus civilian elements, and compatibility of planning tools, processes and cultures. Critical areas for coordination are security, logistics, communications, transportation and information.

The sharing of information is particularly critical for complex emergencies because no single responding entity can be the source of all of the necessary information. Making critical information widely available to responding civilian and military elements not only reduces duplication of effort, but also enhances coordination and provides a common knowledge base so that critical information can be pooled, analyzed, compared, contrasted, validated and reconciled. Civil-military collaboration networks for supporting responses to complex emergencies need to be designed to dismantle traditional institutional stovepipes, to facilitate the sharing of information among civilian and military organizations, to capture lessons learned and best practices, and to provide a common knowledge base for the responding civil-military community of interest.

Experiences and lessons from real world operations collaboration and information sharing suggest that there is a need to create a common culture of trust in information networks and communication between civilian government, military organizations, International Organizations (IO) and non-governmental organizations (NGOs); communications must flow in all directions, all the time; an organization's mission matters; information structures need to be flexible (but not ad hoc); and “lessons learned" need to be learned and improvements institutionalized. The dimensions of communication in support of S&R operations include communication within organizations, between organizations (bilaterally), among organizations (multilaterally, as in a networked community), with local leaders, with and between decision makers, with the media, and among the parties in the conflict. The global revolution in commercial ICT has contributed many invaluable tools and removed many barriers to technical interoperability (Reference 1).

Over the last several years, the Department of Defense (DoD) has become increasingly interested in the challenges associated with the transition from open conflict environments to post-conflict environments. This transition is captured by the term stabilization and reconstruction (S&R). To assist the DoD in preparing for future S&R operations, the Center for Technology and National Security Policy (CTNSP), National Defense University (NDU), has initiated several S&R related studies (Reference 2) including a study of Information Communications Technology (ICT) that not only support S&R operations but also addresses other aspects of complex emergencies such as humanitarian assistance and disaster relief and needs of the civilian elements including US civilian government element (e.g., Department of State, US Agency for International Development), International Organizations (e.g., United Nations, International Commission of the Red Cross), and Non-governmental Organizations (e.g., Mercy Corps, OXFAM, Doctors without Borders). The intent of the study is to capture and document lessons learned and best practices so that future military and civilian participants in complex emergencies can take advantage of the insights that have been extracted from prior experiences. This paper highlights some of the early ICT for S&R ops findings that address ICT systems and data and the challenges related to achieving a collaborative information environment to facilitate civil-military collaboration and information sharing.

THE NDU STABILIZATION AND RECONSTRUCTION STUDY

To assist the USG in preparing for ICT support to future S&R operations, NDU in partnership with ASD NII and DoS (CRS and HIU) and in cooperation with JFCOM has undertaken a study of the information exchange needs and options for the use of commercial

information communications technology to support S&R operations. Participants so far have included US DOD military and civilian elements such as ASD NII, NDU, National Geospatial Intelligence Agency (NGA), Combatant Commands (COCOM), Defense Information Systems Agency (DISA), Civil Affairs (CA), and others and Interagency elements such as the State Department and U.S. Agency for International Development (USAID). The intent is to broaden the participation to other US government organizations, other nations civilian and military elements and to the International Organizations and Non-Governmental Organizations and representative host country elements to the extent possible.

The purpose of the study is to improve the capacity of the stabilization and reconstruction community in a way that makes all of the civil-military players more effective. Additionally, the intent is to propose approaches that allow the United States government capacities, including those of the Department of Defense and State, to work more effectively with other players in stabilization and reconstruction scenarios by enhancing the use of commercial information and information communications technologies and to work more effectively with other nations military and civilian government agencies and with non-governmental organizations, international organizations, and the host country. It is hoped that the effort will serve to help develop a more informed understanding of roles, capabilities and information needs among civilian and military elements participating in S&R operations. The effort has three main thrust areas: information and information exchange needs, systems, and data. Education and training including experimentation and exercises will be considered as well—the civilian and military community need to train together as they work together in the field in support of S&R ops and winning the peace. The end product of the study will be an "ICT Support of S&R Ops Primer." The primer is being designed to capture lessons learned and best practices so that future military and civilian participants in S&R operations can take advantage of the insights that have been extracted from prior experiences.

The contents of the primer are being developed through a sequence of workshops that are being jointly sponsored by the ASD(NII), DoS (S/CRS) and the CTNSP, NDU. Workshops to date have drawn upon experienced military and civilian S&R participants in DoD and selected civilian government agencies (e.g., Department of State). Future workshops will augment the participation with representatives from other USG military and civilian elements, other nations military and civilian agencies, International Organizations (IOs), and Non-Governmental Organizations (NGOs). As a point of departure, the study and workshops have employed the conceptual framework for S&R that was jointly developed by CSIS and AUSA, as published in the CSIS book "Winning the Peace" (Reference 3). The framework tasks are organized around four distinct issue areas, or "pillars": Security; Justice/Reconciliation; Social/Economic Well-Being; and Governance/Participation. The primer will describe both toolkits and best practices for the use of information and information communications technology and will include analysis of information systems, data questions, information requirements, and how to create effective working situations. Austere as well as more robust and mature information environments will be analyzed. Consideration will be given to not only the capabilities of the United States but also the capabilities in other nations and the UN, NGO, international organization and host country communities, and how to improve the ability of all to deal with the humanitarian, governance, reconstruction, and security issues found in a post-conflict environment. It is planned to have the first version of the Primer by September 2005.

The workshops have systematically addressed four interrelated areas: the information needs of key participants in the process (and their associated Information Exchange

Requirements (IERs)); the information and communications systems that the participants need to support those information needs and IERs; the data strategy that the participants should pursue to satisfy those needs; and the education & training (E&T) that is needed to prepare the participants for S&R operations. In each of these areas, the workshop participants are in the process of identifying key Communities of Interest (COIs), characterizing their capability objectives, establishing current baselines, identifying shortfalls, formulating options to mitigate shortfalls, and developing a strategy to move forward. As an example, a gap to be addressed is the need to establish an approach to creating a collaborative information environment to facilitate civil-military collaboration and information sharing. To make these activities tangible, emphasis is being placed on assembling lessons learned and best practices from assessments of real world operations such as the Tsunami Relief Initiative and operations in Afghanistan.

Although the workshop process is still underway, preliminary results are available in each of these areas. For example, in the area of information systems, descriptions of the baseline systems and their relationships have been developed for selected S&R operations and options are being developed to enhance them for future operations. Furthermore, in the area of data, the DoD Net Centric Data Strategy (Reference 4) is being adapted for S&R operations and alternative approaches for implementing that strategy are being explored. As an example, consideration is being given to building upon and extending the multinational Command and Control Information Exchange Data Model (C2IEDM) (Reference 5).

SOME USEFUL DEFINITIONS AND TERMS

A *complex emergency*, as defined by the UN Inter-Agency Standing Committee (IASC), is "a humanitarian crisis in a country, region or society where there is total or considerable breakdown of authority resulting from internal or external conflict and which requires an international response that goes beyond the mandate or capacity of any single and/or ongoing UN country program." .

- *Communications* is a prerequisite for coordination. Without reliable and effective means of communication between military and civilian actors involved in a humanitarian emergency the minimum essential interaction and dialogue can not take place.

- *Information management* is a key component of civil military coordination. In the absence of effective information management within both civilian and military organizations the information shared between these organizations may not reach the right people and information sharing will not have the desired affect of building mutual trust, confidence, respect and basic coordination.

- *Humanitarian Assistance* is aid to an affected population that seeks, as its primary purpose, to save lives and alleviate suffering of a crisis-affected population. Humanitarian assistance must be provided in accordance with the basic humanitarian principles of humanity, impartiality and neutrality. Assistance can be divided into three categories based on the degree of contact with the affected population. These categories are important because they help

define which types of humanitarian activities might be appropriate to support with international military resources under different conditions, given that ample consultation has been conducted with all concerned parties to explain the nature and necessity of the assistance.

> *Direct Assistance* is the face-to-face distribution of goods and services.

> *Indirect Assistance* is at least one step removed from the population and involves such activities as transporting relief goods or relief personnel.

> *Infrastructure Support* involves providing general services, such as road repair, airspace management and power generation that facilitate relief, but are not necessarily visible to or solely for the benefit of the affected population.

- *Civil Military Coordination* is "the essential dialogue and interaction between civilian and military actors in humanitarian emergencies necessary to protect and promote humanitarian principles, avoid competition, minimize inconsistency, and when appropriate pursue common goals." The key elements are information sharing, task division, and planning. Basic strategies range from coexistence to cooperation. Coordination is a shared responsibility facilitated by liaison and common training.

THE CIVILIAN INFORMATION MANAGEMENT ENVIRONMENT

A key element of civilian information management for deployed humanitarian agencies and organizations is establishing and maintaining a conducive humanitarian operating environment (this is sometimes referred to as "humanitarian space"). The perception of adherence to the key operating principles of neutrality and impartiality in humanitarian operations represents the critical means by which the prime objective of ensuring that suffering must be met wherever it is found, can be achieved. Consequently, maintaining a clear distinction between the role and function of humanitarian actors from that of the military is the determining factor in creating an operating environment in which humanitarian organisations can discharge their responsibilities both effectively and safely. Sustained humanitarian access to the affected population is ensured when the receipt of humanitarian assistance is not conditional upon the allegiance to or support to parties involved in a conflict but is a right independent of military and political action (Reference 6).

As per UN General Assembly Resolution 46/182 humanitarian assistance must be provided in accordance with the principles of humanity, neutrality and impartiality.

- *Humanity*: Human suffering must be addressed wherever it is found, with particular attention to the most vulnerable in the population, such as children, women and the elderly. The dignity and rights of all victims must be respected and protected.

- *Neutrality*: Humanitarian assistance must be provided without engaging in hostilities or taking sides in controversies of a political, religious or ideological nature.

- *Impartiality*: Humanitarian assistance must be provided without discriminating as to ethnic origin, gender, nationality, political opinions, race or religion. Relief of the suffering must be guided solely by needs and priority must be given to the most urgent cases of distress.

In addition to these three humanitarian principles, the United Nations seeks to provide humanitarian assistance with full respect for the sovereignty of States. As also stated in General Assembly Resolution 46/182:

> "The sovereignty, territorial integrity and national unity of States must be fully respected in accordance with the Charter of the United Nations. In this context, humanitarian assistance should be provided with the consent of the affected country and in principle on the basis of an appeal by the affected country."

THE MILITARY INFORMATION MANAGEMENT ENVIRONMENT

In modern military forces, communications and information management are components of a broader concept referred to by some forces as Command, Control, Communications, Computers, and Intelligence (C4I). Military communications and information technology systems are designed to ensure that the chain of command, essential control functions, and the intelligence process extend throughout the military force. These are dedicated internal systems and are among the most vital systems in a military force. If an adversary can disrupt, damage, or destroy these systems the ability of the force to function and survive is at risk (Reference 6).

In order to protect the integrity of these systems access to the communications and the information management systems of the military are carefully controlled. Levels of access to both communications channels and the information in the system are used to protect the system itself and the information and data that flow through the system. Access to information is managed through a system of classification. All military personnel have security clearances that determine the level of information to which they have access. Within a level their access is further restricted by their "need to know". In other words, they are only given the access to the sensitive information that they need to know in order to perform their jobs.

Military personnel are consistently reminded to maintain "information security" and "operational security." The later refers to the protection of the intentions, plans and capabilities of the forces. Thus, information is linked to the security of the force and denying potential adversaries knowledge about the force. As a result, military personnel, as a matter of policy and training, are hesitant to share information. Access to facilities where this information is collated, shared, or disseminated is strictly controlled.

Military commanders, even at the highest level, have limited authority to share classified information with personnel who have not been vetted. Information received from intelligence agencies is often classified and controlled by the intelligence agencies. Commanders in the field normally have no authority to share this information beyond the approved addressees, even within their own organizations.

Among the most important of controlled facilities is the "operations center" in a headquarters or the "command post" at the lower tactical level. These locations are critical nodes in the C4I system. Access to these locations is always restricted and in combat operations the military forces will attempt to keep these locations secret. Unescorted access to these areas is rare, even for personnel with the appropriate level of security clearance.

In situations where the military recognizes the need to share unclassified information with humanitarian and other civilian actors, this information will normally be shared via a Civil Military Operations Center (CMOC) or in NATO parlance, a Civil Military Cooperation (CIMIC) Center, the dispatching of military liaison officers, or via an electronic bulletin board, Internet web sites/portals and exchange of e-mails.

S&R OPS: A COMPLEX OPERATIONAL ENVIRONMENT

The decision to intervene in a conflict is political. The military mission in support of the intervention reflects the political process. The primary mission of the military is to create a safe and secure environment so that civilian government agencies, International Organizations (IO), and Non-governmental Organizations (NGO) can conduct humanitarian assistance and assume appropriate responsibilities for civil policing, justice, governance, economic and related recovery and reconstruction and nation building activities. The military is not there to do the jobs of the civilian agencies and organizations; however, since provision of adequate security is one of the most basic and immediate needs in a post conflict environment, the military, as the principal representative of the intervening power, are obligated to provide security (military and civil) and appropriate humanitarian assistance, governance, restoration of essential services, and other reconstruction assistance until the security environment permits adequate civilian access to perform their duties. The civil-military mission is to enable the host country leadership to establish the necessary capacity to manage governance, rule of law, reconstruction and economic recovery.

In these complex environments, information expectations between the military and the civilian elements must be carefully managed. The military has been repeatedly told that the humanitarians have superior knowledge of the humanitarian situation, culture, language, and the population in general. Humanitarians have grown to believe that the vast intelligence capabilities of modern states and militaries are available to all military units. In ordinate expectations lead to the belief that information is intentionally being withheld and that erroneous information was intended as disinformation.

Achieving a shared civil-military vision, managing shared expectations, and facilitating collaboration and information sharing is key to achieving unity of effort in complex emergencies. The challenges of civil-military information management, collaboration and information sharing in support of such emergencies are not a technology issue. Technology is an enabler. The challenges are political, organization culture differences, lack of mutual

trust, confrontational attitudes and lack of adequate civil-military social networking. The military objectives are driven by political objectives. Legitimate humanitarian actions are driven by concern for the population. When the creation of a stable political environment, with full respect for human rights is the political objective, potential for cooperation is high. *When the population is a military target, cooperation is virtually impossible for humanitarian actors.* Experience suggests that civil-military collaboration, coordination and information sharing has been and continues to be problematic

As noted, technology is an enabler and some progress has been made in establishing multinational collaborative information environments for coalition military operations. For example, the U.S. government secure multinational military information network—the Coalition Enterprise Regional Information Exchange System (CENTRIXS) (Reference 7) has been employed to create multilevel secure virtual private networks (VPN). Although the U.S. military controls the release of information and network access privileges for the non-U.S. military elements approved to receive and share information over these networks, an environment is created that facilitates collaboration and information sharing. A similar formal arrangement does not exist for sharing information among civil-military elements responding to a complex emergency. An informal arrangement, the Internet, does offer the opportunity and more recently, has been used to create some limited collaborative arrangements to share civil-military information.

Figure 1: The Post-Conflict S&R Operations Challenge.

During the transition from combat operations to stability and reconstruction operations, it will be necessary to adjust the force structure and capabilities. In today's high tech operational environment, however, there will likely be no distinction of phases (see Figure 1) but a blurring of the phases with combat operations being conducted in parallel with civilian and military stability and reconstruction operations—this is the case in Afghanistan and Iraq. There will be a need to move from a heavy combat force to a force configured to operate in

urban areas. Force augmentation or adjustments will need to address coexisting civilian security, counter insurgency, counter terrorism, and organized crime security and law enforcement needs. Additionally, stability and reconstruction activities such as humanitarian assistance (food, clothing and shelter), restoration of emergency services (fire and rescue, hospital, ambulance), infrastructure repair (power, water, transportation, communications, sewage), governance, health care services, education, and other quality of life needs including jobs for the unemployed need addressed.

If one looks at the entire operational spectrum depicted in Figure 1, both military and civilian resources are employed across the full spectrum. The military has its core competencies but so do the civilian agencies. Trying to sub-divide the spectrum accomplishes little, and instead reinforces the military view that there are easily discernable and distinct thresholds that separate civilian and military operations.

It should also be recognized that the civilians are likely to be present before the military is called in and will remain long after the military has departed. There are a number of transitions that will occur over time, and ultimately the intent is to handoff complete self-sustaining peace to the affected nation. Recall that even in unique conditions that existed in Iraq before the US military invaded, the UN had inspectors and World Food Programme staff operating in country. In Afghanistan, the US military forces were introduced to their Afghan coalition partners by the CIA operatives who were present long before the military deployed, and because of our lack of coordination with the World Food Programme, an organization that was operating in country for more than 15 years, we bombed some of their warehouses containing the food they were distributing to the local population. The military must plan their "passage of lines" into on-going civilian operations carefully if they want to exit gracefully. Again separation of upper end and lower end military operations has little utility other than continuing the compartmentalization of what is in fact a continuous spectrum involving both military and civilian partners.

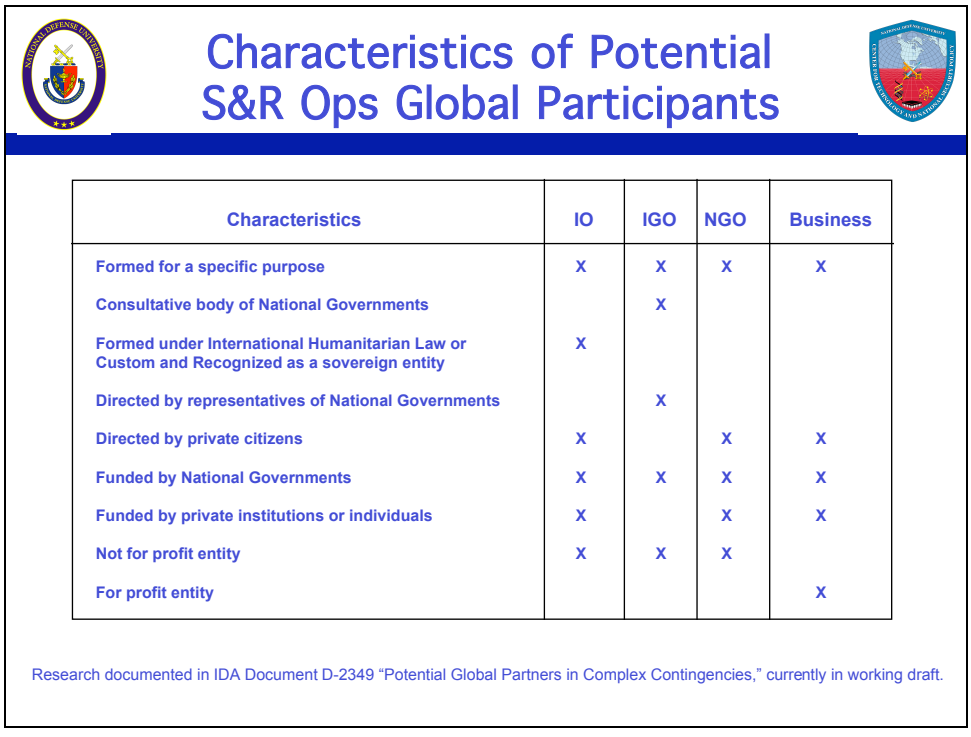
What really occurs in today's operational environment is a coalition of coalitions operating in the affected nation. Even during the cold war era, the host nation authorities planned to operate where they could while combat was ongoing, and when it was terminated, they assumed responsibility for restoring the nation. In today's environment these coalitions exist throughout the full spectrum of operations beginning with peacetime engagement — e.g., security cooperation (DoD and DoS), developmental programs (USAID, DoJ, and other agencies), global war on terrorism (Treasury, Justice, Homeland Security, DoD, DoS, etc.). A crisis may erupt prompting actions to be taken to remedy the situation. If conflict occurs, there follows a post-conflict stabilization and reconstruction phase. All crises, however, do not necessarily result in military force as the solution.

The economic crisis in the Pacific-rim countries a few years ago is an example of a situation where the military was not involved, but instead, the crisis was resolved by civilian agencies. The key points are that these civil and military coalitions will vary as tasks change and resources are adjusted to accommodate circumstances, and all partners must be involved with the planning and execution of operations throughout the full spectrum of operations. To try and separate these interactions and the need for coordination seems counterproductive. Moreover, the desired end state is a "political-military" solution, not merely a military solution. Consequently, in the case of the US, the military operation plan should be an annex of the Interagency Political-Military Plan, along with the annexes of the other involved agencies, and the military plan should recognize not only friendly military forces but also the

civilian forces that participate in the operation. Otherwise, it can be perceived that the military runs the interagency and is not part of it (Reference 8).

CIVIL-MILITARY PARTICIPANTS

There are numerous civil-military participants (Figures 2 and 3) on the stability and reconstruction landscape with good intentions to help but come with different capabilities, agendas, accountability, and expectations and multiple independent lines of authority directing their activities. There is a general lack of mutual understanding of roles and capabilities and the ability to communicate and share information among the civil-military elements is problematic. The military commander and civilian authorities have little control over many of the participants. Absence of "trust" is a fundamental source of tension among the civilian and military participants as well as the local population and leaders. Therefore, understanding the roles, relationships, capabilities and motivations and information sharing needs in this complex environment are key to success. Managing expectations is key as well and actions need to support words. Early introduction of information communications technology to facilitate collaboration and information sharing among the civilian and military elements is also key to the success of not only the security aspects but to the successful capacity building needed to rebuild governance and infrastructure of the host nation and to also facilitate economic and social well being recovery as well.



Characteristics	IO	IGO	NGO	Business
Formed for a specific purpose	X	X	X	X
Consultative body of National Governments		X		
Formed under International Humanitarian Law or Custom and Recognized as a sovereign entity	X			
Directed by representatives of National Governments		X		
Directed by private citizens	X		X	X
Funded by National Governments	X	X	X	X
Funded by private institutions or individuals	X		X	X
Not for profit entity	X	X	X	
For profit entity				X

Figure 2: Characteristics of Potential S&R Operations Global Participants.

In order to effectively promote their respective missions, the military and the civilian government agencies, IO, and NGO organizations must have their own spheres of operation, or "spaces," and information integrity. They need to collaborate in working toward the common goal of protecting and helping the local population and leaders when their needs and

objectives overlap. The civil-military elements must share suitable, protected mechanisms for exchanging information.

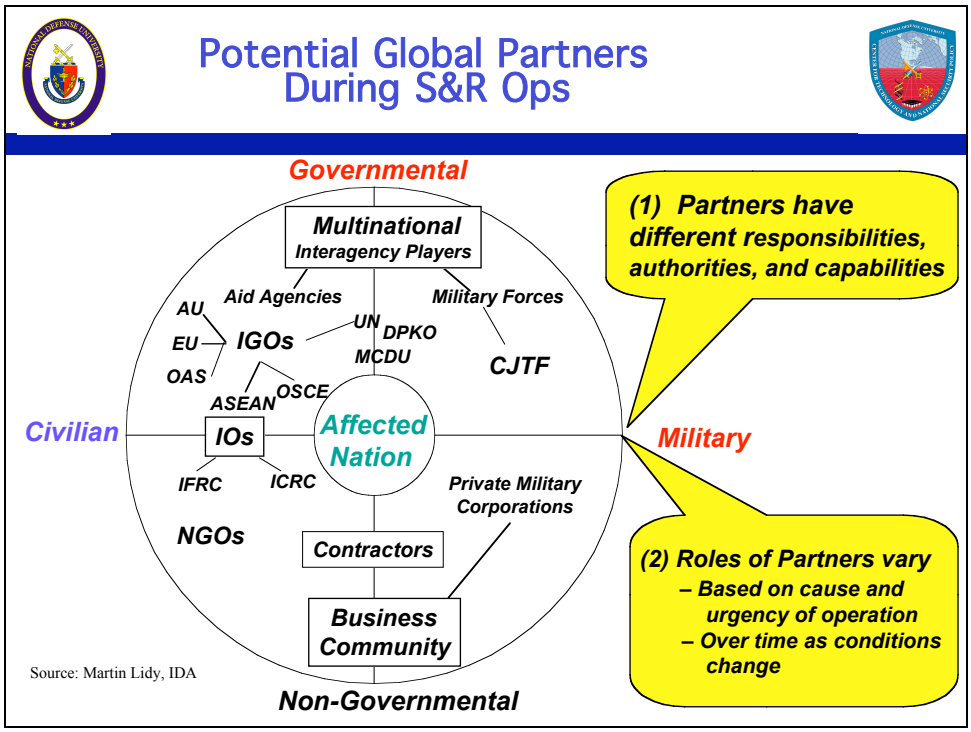


Figure 3: Potential Global Partners During S&R Operations.

ICT SUPPORT CHALLENGES

Civilian and military communications and information systems supporting stability and reconstruction operations tend to be stove-piped with limited coverage and capacity and little interconnection of the deployed military and civilian systems. Commercial Internet becomes the de facto information network that informally links civil-military participants but this is not enough. There are other non-technical challenges such as language differences, restrictions on release of information and organization culture differences that contribute to limiting the ability to effectively conduct civil-military information management and hence, create a collaboration and information-sharing gap. Policymakers from both sides need to evaluate the necessities and realities that face them in the field and manage their respective needs for information integrity and the means to cooperate. Commercial ICT offers a means to create a civil-military collaborative information environment to facilitate collaboration, cooperation and information sharing.

Effective civil-military collaboration, coordination and information sharing is essential to achieve unity of effort, especially in an environment where no one civil-military element is really in-charge of the over all operation. Even for the coalition military with a highly structured command arrangement, there are shadow and independent national level reporting lines of command of the troop contributing multinational military elements. For operational security reasons, there is a continuing reluctance on the part of the military to share information with anyone other than military—especially with multinational political bodies,

civilian organizations, IOs, NGOs and host country leaders. Even for military-to-military sharing, strict need-to-know rules are applied. The IOs and NGOs desire to maintain the perception of neutrality and this has adversely influenced their willingness to work with the military and share information with them. This challenge has been given sharper focus in recent real world operations, such as Afghanistan and Iraq, since they are required to operate in increasingly hostile environments and the respect accorded humanitarian actions has eroded significantly—security is a major concern since they have become targets of hostile actions as well.

The civil and military challenges span differences in culture, language, organization, training and education, doctrine, CONOPS, Tactics, Techniques, and Procedures (TTP), planning and analysis and M/S tools, and communications and information systems capabilities to facilitate the planning, execution, and assessment of S&R courses of action. Old business models and restrictive policies continue to be applied to support the needs of the new and highly dynamic collaborative information environment of today's S&R operations. Informal and unofficial personal relationships play an important role in achieving the sharing of information but this makes it difficult to serve a wider audience and to institutionalize as a standard process. As a result, sneaker nets and face-to-face meetings become the preferred means to collaborate and share information in the complex and austere information environment that accompanies S&R operations.

INFORMATION AND INFORMATION EXCHANGE NEEDS

The informational needs of military and humanitarian actors are different even when they involve the same subject or topic. This often requires explanation of what the data will be used for and what the implications are for humanitarian operations. Assuming that a formal request for information has been established the following should be considered when explaining the needs.

- Common terms used by the military and civilians often have different meanings. For example, the term sector means a geographic area of responsibility for a military organization while it is a functional area such as water/sanitation, food, shelter, etc. for the humanitarians.

- The urgency of the need for humanitarian data may not be readily evident to the military. When the request is passed to those who must collect the data, the priority may be altered due to other informational needs of a higher priority. One should try to avoid depending on the military for data that is time sensitive and has not been shared before.

- When requesting data or information from the military it is normally better to state the need in terms of the decision that must be made instead of the raw data that is being used to make the decision. For example, imagery of mountain passes is of use to humanitarians in determining when passes might close. Instead of asking for imagery, ask for a forecast of when the passes will close or no longer be accessible by a particular mode of transportation.

Dennis King, US Department of State, Humanitarian Information Unit, in his paper (Reference 9) titled "Humanitarian Knowledge Management" notes that identifying information and information exchange needs is not easy. Natural disaster, humanitarian emergencies and S&R operations are, by their very nature, complex and dynamic situations. They are multi-sectoral and multi-disciplinary, incorporating both the physical and social sciences. Information is constantly changing, comes from a multitude of sources and is often incomplete or contradictory. In some cases, there is an overload of information and, in other cases there are complete gaps in what is known. Collecting information is often difficult, if not impossible, because of inaccessibility to the affected areas due to natural hazards, lack of a safe and secure environment or government restrictions. Furthermore, much of the "available" data are actually estimations, based on selective sampling or extrapolations of dated statistics, such as census information, projected growth rates, and proxy indicators.

There is also a certain amount of misinformation and disinformation generated about complex emergencies. Governments and aid organizations may publish inflated or high estimate data about a complex emergency in order to appeal for higher amounts of international assistance. Furthermore, participating civil-military elements may purposely conceal information about the situation in a country that in turn may mislead the international community. Decisions about providing assistance in response to complex emergencies often must be based on the best available information and insufficient knowledge about the situation.

Another challenge is the inconsistent use of standardized meta-data when collecting and providing S&R ops information. All incoming and outgoing data and information should include the source and the date or time-stamp, so that other users can determine the credibility and currency of the content. Likewise, it is important to make sure that ambiguous terminology is clearly defined and methodologies and indicators explained, so that others can use the data and information correctly. Finally, data and information should be geo-referenced to include the latitude/longitude, geo-code, gazetteer place name, administrative unit, etc., so that the data can be entered into a Geographic Information System (GIS) and mapped. If these standards are followed, data and information provided by many different civil-military organizations can be effectively pooled, compared, contrasted, validated and used for analysis, mapping and operational activities.

WHAT DO S&R ORGANIZATIONS NEED TO KNOW?

In any complex emergency, there are certain questions that the civilian and military response organizations want answered. Certain background and situational information is needed by all S&R organizations: Military, civilian government, IOs, NGOs, UN agencies, and donors. There are other types of information that are organization specific and needed by different personnel within these response organizations. For example, organization policy makers want "big picture snapshot" analysis in order to understand the issues, to make decisions on providing assistance, and to be alerted to problems and obstacles. Field personnel and project and desk officers in S&R organizations, on the other hand, need more detailed operational and programmatic information in order to plan and implement humanitarian assistance and reconstruction programs.

Most S&R information needs can be divided into the following basic categories:

- *Situational awareness*: S&R organizations need to know the latest about the situation on the ground and information about the conditions, needs, and locations of affected populations.

  > What is the latest/current humanitarian and reconstruction situation in the country?

  > What are the most recent severity indicators? (death tolls, mortality rates, malnutrition rates, economic impact, infrastructure damage, etc.)

  > Who are the affected populations (refugees, IDPs, children and other vulnerable groups, resident populations, etc), how many are there, and where are they located?

  > What are the conditions and humanitarian needs of the affected populations?

  > What is the assessment of damage to infrastructure? (transport, buildings, housing, communications, etc)

  > What is the latest/current security situation in the affected areas of the country?

- *Operational/Programmatic*: Information necessary in order to plan and implement humanitarian assistance and reconstruction programs.

  > Where are and what are the conditions of the logistical access routes for delivering humanitarian and reconstruction assistance?

  > Who's Doing What Where? What assistance organizations are working in the country, what are their programs, what are their capacities and where are they working?

  > How is the host country/government responding and can it provide more?

  > What are the programmatic/financial needs of the responding organizations?

  > What and how much is being provided to the response organizations and who are the donors?

- *Background*: Background information is needed to provide knowledge about the unique history, geography, population, political and economic structure, infrastructure and culture of the country. Baseline data are also necessary for assistance organizations in order to be able to compare the emergency situation and conditions to previous normal conditions.

  > What is the country's population (national, province/state, city/town) and its composition (ethnicity, religion, age cohorts, urban/rural, political, etc)?

> What is the geography of the country?

> What are the country's past disasters and natural hazards?

> What are the most recent annual baseline health indicators for the population? (Crude Mortality Rate, Infant/Child Mortality Rates, HIV adult prevalence, malnutrition, etc)

> What are the annual economic indicators? (GDP, GNP, agricultural/food production, staple food prices, etc)

- *Analysis*: Humanitarian and reconstruction information needs to be interpreted in context and related to other thematic information. Analysis can include evaluations of issues and responses, projections about the future, and recommendations for policies and actions.

> What are the causes and contributing factors of the emergency?

> What are the constraints to providing humanitarian and reconstruction assistance? (insecurity, inaccessibility, government interference, etc)

> How effective are humanitarian and reconstruction assistance programs and responses?

> What are the future impacts of the emergency?

> What are the options and recommendations for action?

WHERE CAN RESPONDING ORGANIZATIONS FIND WHAT THEY NEED TO KNOW?

The emergence of the Internet in the last ten years has revolutionized the availability and dissemination of humanitarian and S&R related information. Email has greatly facilitated the transmission of information between the headquarters of the humanitarian and S&R response organizations and the personnel, teams, and programs located in the affected countries. The World Wide Web provides a vast, virtual library of information to users with Internet access. At the same time, the Internet has added to the overload of information and the increasing difficulty in locating, extracting and verifying the answers to the critical questions—information and knowledge management. There are also information assurance challenges—trust and self-policing on information on the network is the norm. No one organization element is responsible for assuring the quality and integrity of information placed on the network and no standards are employed for collecting and populating the various web sites which adds to the challenges of sharing information.

Situational information is reported in the news, but more directly in the situation reports and field assessments from the response organizations working in the affected countries. These organizations also produce and issue appeals, proposals, and project monitoring documents that provide operational and programmatic information. Useful

background/baseline information can be found in country profiles, maps, databases, and chronologies. Analysis is derived also from evaluations, lessons learned, research studies and policy recommendations.

Not everything that S&R organizations need to know, however, can be found in databases, documents and visual products. There is also tacit knowledge that is usually not documented, but derived from expertise, collaboration and field experience. This knowledge is often imparted from briefings, discussions, and first hand observation. "Seeing it for oneself" adds a great deal to one's knowledge and understanding of any humanitarian emergency.

There are a large number of sophisticated intelligence collection systems available to military. Most are designed for collection of information relevant for military operations and some are extremely classified and the information collected by these sources is carefully controlled by the military. Most information relevant and available to humanitarians will be collected on the ground.

The military is more likely to be effective in gathering data about tangible measurable things such as the length of an airfield and the number of structures in a village that have their roofs intact. They seldom have the skills to make more than broad observations about issues such as food security, access for ethnic minorities, etc.

In many militaries deployed outside of their own countries direct interaction with the population is limited either by policy, regulation, or tactics. Effective interaction, when it is permitted, may be further limited by language, culture, or distrust. Much of the information collected by the military regarding the population is collected by junior soldiers on patrol. In some militaries there are dedicated trained personnel who interact with the population and conducted CA/CIMIC patrols to collect or verify data. It is important to know how the data was collected and whether or not it has been verified before taking action.

ICT RESPONSE CHALLENGES

Effectively collecting, compiling, analyzing and disseminating timely and relevant information is one of the primary challenges for S&R response operations. Better information and knowledge management can improve the effectiveness of S&R response and assistance elements. The faster S&R civil-military response organizations can identify, collect, analyze and disseminate critical information, the more effective the response becomes.

The larger civil-military elements responding to a complex emergency will bring with them the necessary ICT to support their mission needs, see Figure 4. The military will respond by implementing both classified and unclassified networks to support their command and control, intelligence, logistics and other operations and information exchange needs. Military access to the Internet will be provided and web sites related to the emergency will appear on both the classified and unclassified networks. The large civilian organizations, such as the UN, deploy a significant commercial ICT infrastructure as well to support their assistance operations and information exchange needs. They too create web sites to share information such as situation awareness, maps, GIS products and other assistance related information. Other civilian organizations deploy with a lesser ICT capability but they too

access the Internet and create web sites to share information. And Bloggers now populate the Internet with information on the crisis.

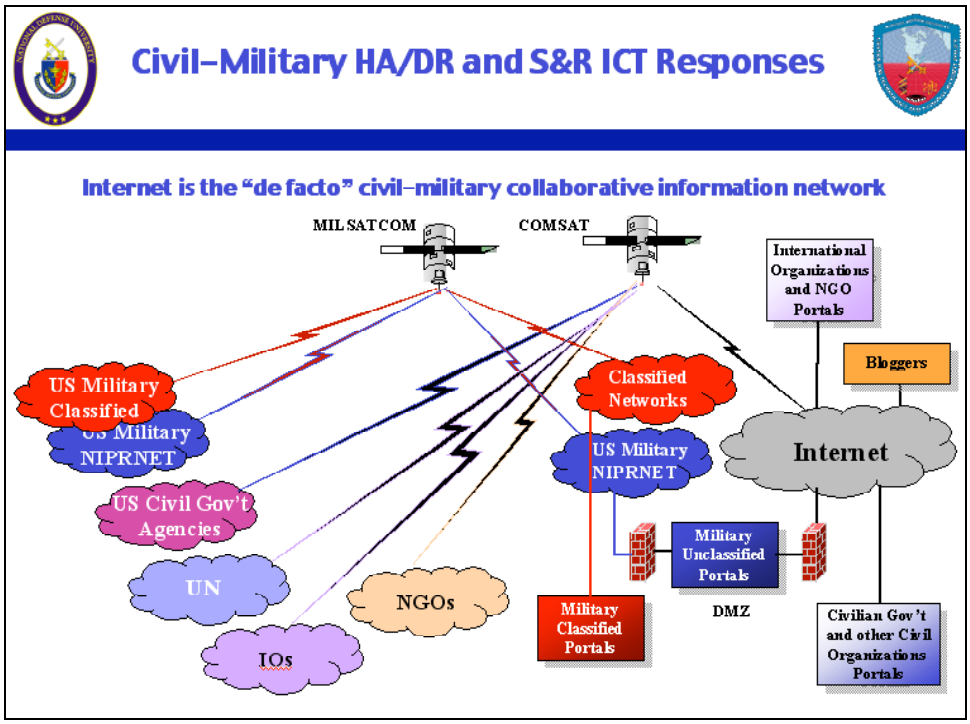


Figure 4: Civil-Military S&R ICT Responses.

Among all of the ad hoc civil-military ICT deployments, one capability emerges that is common and used extensively by both the civilian and military participants and that capability is the Internet—the "de facto" civil-military collaborative information environment used to collaborate and share information. Additional commercial ICT capabilities are becoming more pervasive as well and both civilian and military elements deploy with and use PDAs, cell phones, commercial handheld line of sight radios and HF, VHF, and UHF radios to communicate during S&R operations. To the extent possible, participants also use the public switched telephone systems, cellular networks and commercial satellite systems to communicate and access the Internet through local ISPs if they exist and/or remotely via satellite phone access.

Obviously, in austere public ICT environments, the ability for all responding elements to effectively access and communicate may be extremely limited and this makes it difficult to establish and maintain connectivity with the Internet and to communicate in general among the participants. On the other hand, the more ICT capable civilian and military elements responding to a crisis establish forward deployed ICT capabilities and create information centers such as the military civil-military operations centers (CMOCs) and the UN humanitarian information centers (HICs) to facilitate the sharing of information with other responders and with host nation political and business leaders and with the local population including establishment of Internet cafes to provide Internet access to locals and those civilian responders needing access to the Internet. The more ICT capable elements can also offer services and access to others less capable. The key is leveraging the collective capabilities by smartly bridging the seams between the stove-piped systems deployed.

There is no agreed overarching CONOPS and System Architecture for ICT support to S&R ops. Furthermore, civil-military community leadership is lacking among the participants to pull together the disparate capabilities and create and manage a federated ICT network and distributed information and knowledge environment. It's largely an ad hoc event that employs "old boy" networks and personal contacts to create basic things such as a phone directory, email listing, radio nets, and on the ground shared situation awareness. Technology is not the issue—technology is an enabler. The challenge is leadership and the "will" of the civil-military elements participating to take the necessary actions to create a collaborative information environment to facilitate collaboration and information sharing. The ICT capabilities and know how exists to create a federated network forward and a distributed information environment to support S&R ops information exchange needs.

A family of flexible, scalable and rapidly deployable S&R Civil-Military ICT capability packages can and are being created using off the shelf commercial ICT products and services and Internet portals and metadata repositories can and are being created and employed to build a distributed information and knowledge network to satisfy the needs of the civilian and military responders to S&R ops. Figure 5 illustrates a de facto S&R ops civil-military ICT architecture that emerges from what is done today and suggests that this can be a reality for future operations through smarter use of the capabilities deployed by today's responders. There are some ICT network and system management and information assurance and information and knowledge management challenges to be overcome but these are solvable if the cultural challenges can be overcome. The civil-military community needs to come together to make this happen.

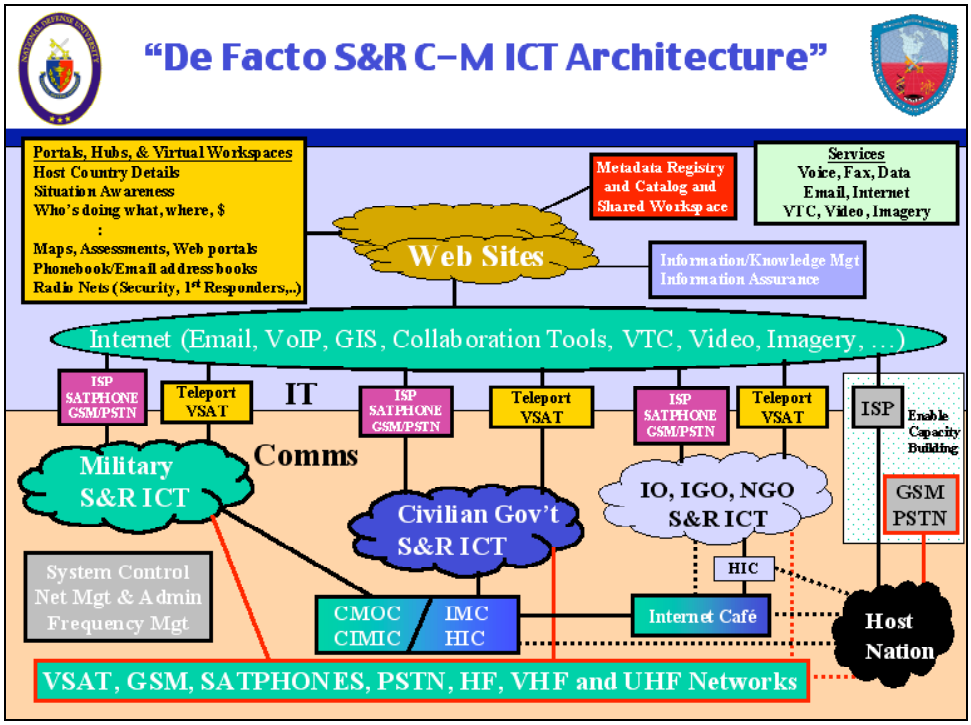


Figure 5: A de facto S&R operations civil-military ICT architecture.

ICT SYSTEMS FOR S&R OPERATIONS

It is a reasonable assumption that the national telecommunications infrastructure of the country for which an S&R operation takes place will likely not have sufficient capacity and coverage to support the S&R operational needs of the military and non-military participants. Hence, these elements, including IOs and NGOs, will bring their own capabilities and leverage the use of local telecommunications, commercial SATCOM services and Internet service providers to the extent possible and available.

Long-haul, high capacity systems such as fiber and commercial SATCOM will be used to extend coverage and data pipes needed to support the forward deployed military C2, Intelligence, and logistic support needs as well as civilian element humanitarian and reconstruction assistance needs. For example, USAID/OFDA/DART fly away ICT packages and UN deployable ICT capability packages use commercial SATCOM extensively to connect headquarters organizations with the field elements. NGOs are now employing small ICT packages that rely on transportable satellite terminals such as the Inmarsat family of mobile terminals to access the Internet and global telecommunications services. Commercial ICT capabilities are becoming pervasive and hence, becoming a part of both the military and non-military inventory of deployable capabilities.

Although commercial SATCOM capabilities provide wide area, spot and global access coverage for deployable ICT capability package use, the coverage and capacity can be limited especially in the remote end user areas and responders should therefore not expect wideband services at the outset of operations. The coverage limitations can also result in poor performance due to low bandwidth access and intermittent coverage and overloads of the civil telecommunications and satellite infrastructure not designed to absorb the surge can occur due to high usage demands of responding elements and this can have significant impact on end user performance.

BASELINE ICT SUPPORT

A survey of the ICT capabilities employed by military, civilian government, IOs and NGOs suggests there is a high degree of commonality of commercial ICT capabilities used by them. NGOs that used to show up with a pencil and note pad now arrive with at least a cell phone and some have laptops while others arrive with satellite phones that can be used to connect to the Internet—not high speed but good enough to communicate and share basic information. The non-military elements use Internet web sites and portals extensively to share information and such web sites are used by the military as well for sharing information with non-military elements. Cell phones are carried by almost everyone entering the S&R area of operation. Satellite phones have gained popularity for use in austere environments to gain near real time access to the Internet and VSAT terminals are employed extensively to create wideband access arrangement for local area networks. Wireless as well as fixed local area networks with collaboration tools are being use to create collaborative information sharing environment.

Figure 6 illustrates the degree of overlap of commercial ICT capabilities employed by participants in S&R ops. It also illustrates the high degree of stove-piped systems that get

deployed that with some smart systems engineering could be integrated into a federated network to create a collaborative information environment to support civil-military communications and information sharing in support of S&R operations.

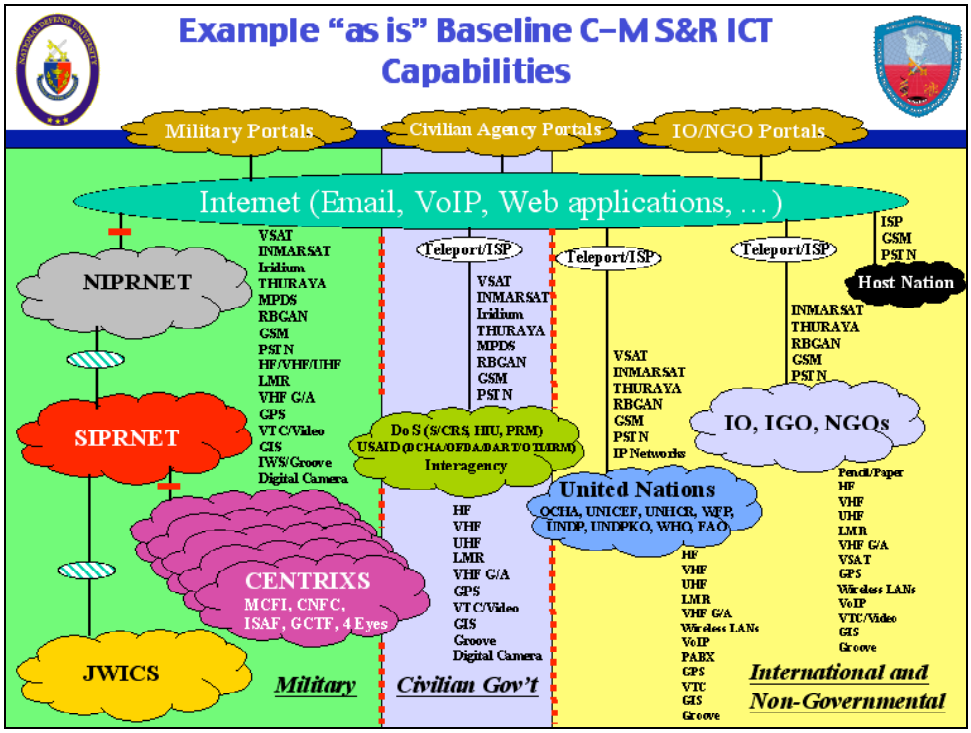


Figure 6: Example "as is" Baseline S&R ICT Capabilities.

A REAL WORLD EXAMPLE

The civil-military response to the South Asia Tsunami employed smart use of the power of commercial ICT and web technology to support a major disaster but in spite of the successes there were ICT networking and information management challenges. Although the response was better than has been done in the past, many of the challenges remained the same—cultural, legal and procedural. Figure 7 illustrates the ICT and distributed information environment created by U.S. government elements to support the communications and information sharing needs of the civil-military elements responding to the disaster.

GSM cell phones were provided by the US military elements to international IO and NGO responders and local response personnel to facilitate communications and coordination. It turned out that the cell towers in some regions were on mountaintops and not destroyed so there was cellular coverage. However, demand for cellular access and use exceeded the network design capacity causing degradation in service during critical phases of the operation. Hotels not in the immediate disaster area had phone service as well as wideband Internet access and these capabilities were used by deployed civilian headquarters elements of relief organizations. The US military also gave out wireless laptops to facilitate collaboration and information sharing and wireless and wired local area networks were created and linked to the Internet via commercial SATCOM using VSAT terminals and existing Teleport access arrangements. Here again, there were challenges in deconflicting

multiple wireless networks independently established in the same area of coverage. Satellite footprints and limited bandwidth in the area of coverage were a problem limiting the performance of satellite access to the Internet and other communications demands. Dial-up ISP access for Internet service was also possible in some areas but slow and extremely limited in bandwidth. Other satellite phones such as INMARSAT, THURAYA, and IRIDIUM were used for communications and limited bandwidth access to the Internet. Downloading files from the Internet proved to be slow and difficult at times. There was a high demand for maps and imagery and attempts to download these from Internet sites proved to be difficult, especially when the files were very large and the communications pipe small. It would have been easier and in some cases faster to produce CDs and hand-deliver them to the field.

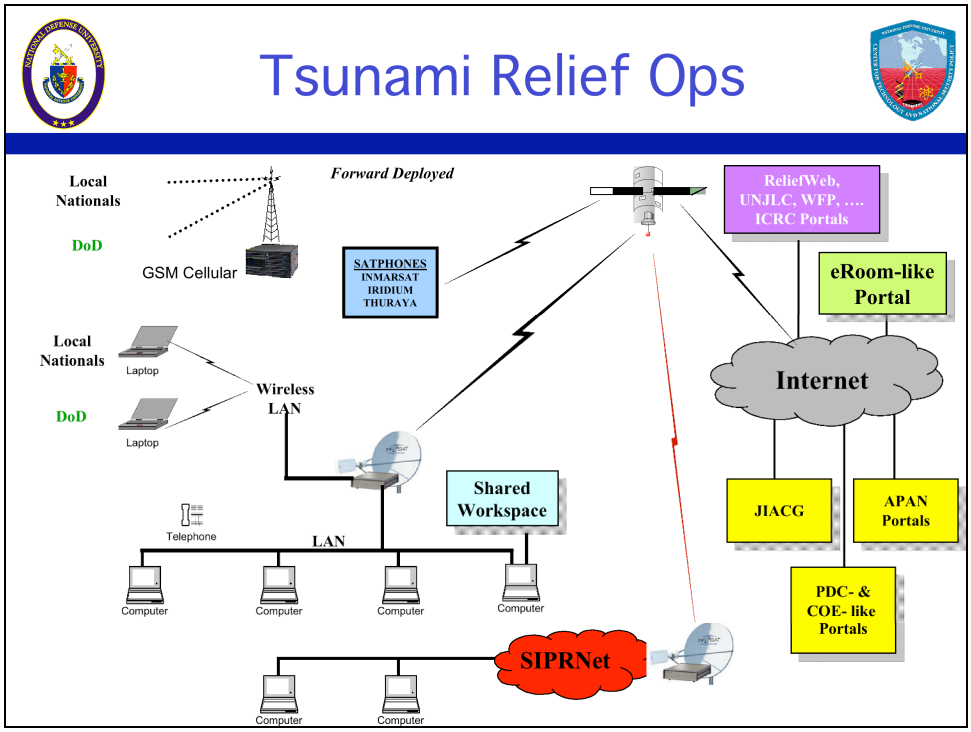


Figure 7: Tsunami Relief Operations.

Collaboration tools such as Groove and others were used. A virtual CMOC was created on the U.S. Pacific Command Asia and Pacific Area Network (APAN) and hot links were created to UN portals (e.g., WFP, UN Logistics Center and ReliefWeb) and other Tsunami relief information sources such as the ICRC. The Pacific Disaster Center provided imagery access and the Pacific Center of Excellence provided information and assessment services via their portal. The State Department Humanitarian Information Unit established a collaborative environment on their eRoom to facilitate Interagency sharing within the Washington DC area and to collect lessons learned. NGA made imagery and other analysis available though various U.S. government portals. The US military extended its SIPRNET capability to support intelligence and other military command and control and logistics needs on the ground.

In spite of improved use of commercial ICT, the world community response to the Tsunami repeated many of the disjointed approaches to disaster and humanitarian assistance that have been experienced in the past, particularly with respect to data/information

management. Although the need for data and information on the Tsunami event (for assessing damage, planning relief and recovery efforts, delivering aid) was immense and immediate, the community's response was once again slow and disorganized and somewhat uncoordinated. Repeatedly, the response community finds itself unprepared to deal with some of the largest issues of information management (the ability to locate and acquire data quickly, determine its freshness, and the ability to share it with others) thus hampering or delaying the ability to generate necessary information products for the people who are executing operational activities.

Many of the same issues that have plagued the civil-military response community in past events were once again experienced:

- No to limited "shared informational awareness" to enable everyone to understand what data/information are/will be available, what has been or needs to be done to it, who needs it, or who has it.
- Multiple organizations producing the same information products.
- Organizational use of deprecated data (i.e. "old" data).
- Stove-piped and incompatible systems that were unable to share information with others because of either format or bandwidth/connectivity issues related to operating in austere ICT environments.
- Numerous applications were incompatible with data/information formats of others.
- Pushing large amounts of data to multiple locations, multiple times.
- End users who's access bandwidth could not support downloading large data files such as maps.
- Hard for those on the ground to find needed information (i.e., lack of understanding of what was available and how to access, information overload).

While there were a number of respected organizations generating the necessary information and products, the inability to leverage existing data to current situations limits the ability to effectively respond to the crisis. The proprietary and unknown contents of the various systems, often secured, caused information assurance concerns reducing the "shared situational awareness" across the community. Additionally, there were multiple collaboration tools (or collaboration rooms) used that were developed independently and to different standards, each using a different software package, and each unable to share information with the other. Few of these tools were developed with the end-user in mind, especially where limited connectivity and low bandwidth concerns in the field are the norm for austere ICT environments.

As noted, technology (both hardware and software) is available today to allow many of these problems to be solved, quickly. However, the biggest roadblocks continue to be cultural and institutional: getting people and institutions to work together. Because this involves

changing operational processes and cultures, these are perhaps the largest and most challenging hurdles yet to be overcome.

CREATING A COLLABORATIVE CIVIL-MILITARY INFORMATION ENVIRONMENT

There is a need in the S&R phase of operations to create a common communications culture in order to increase trust and improve the ability to collaborate and share the information necessary to achieve both the civil and military goals. This must be done without undermining International Organizations' and NGOs' neutrality and the military's sensitivities to exposing operational security information. Even sensitive but unclassified information needs some level of protection. Who's doing what where in terms of reconstruction is useful for resource allocation and managing the efforts but it can also be a target list for insurgents who want to disrupt success and influence public opinion and create fear. The creation of a collaborative information environment (CIE), see Figure 8, is a fine line to walk; but it can be done if everyone is sensitive to one another's concerns. It is certainly not a technology issue. Technology is an enabler.

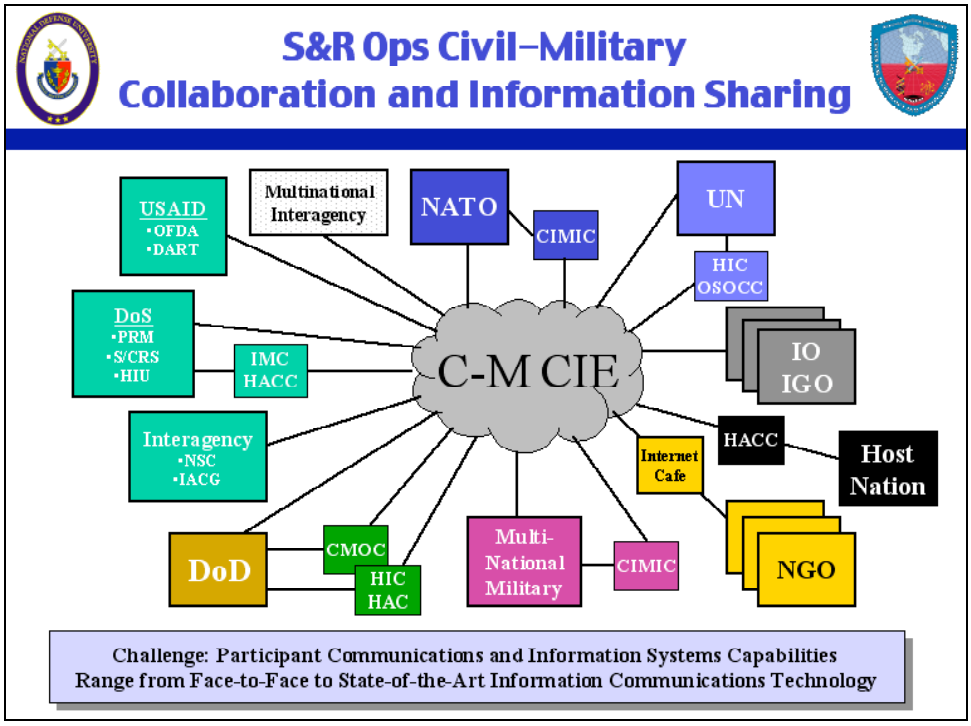


Figure 8: S&R Operations Civil-Military Collaboration and Information Sharing.

The ability to provide a ubiquitous ICT network with the agility and adaptability for authorized participants to "plug and play" to obtain the right information at the right time from anywhere in the world or on the S&R landscape means the CIE needs to accommodate the "agility and adaptability" necessary to respond effectively to event-driven, high-tempo, short-time scale, uncertain, diverse and dynamically varying operations imposed by the needs of an unpredictable and complex S&R environment. The CIE needs to be able to mediate flexible and timely interaction between "come-as-you-are" heterogeneous systems and

information databases to provide agile C2, shared situation awareness, and improved interoperability and collaboration to support coherent civil-military operations. In the event that S&R operations overlap with combat operations, there is a need to be able to provide a virtual presence in the hostile area through reachback to analysts and subject matter experts in rear areas. Likewise, there is a need to accommodate distance learning both for those in hostile areas and for those in pre-deployment training who are geographically dispersed and can not be physically brought together for training purposes.

There is a need for the military and other agencies that produce classified information products to be able to more easily partition and declassify information so that it can be released to coalition military partners in some lesser level of classification and unclassified versions to non-military elements such as NGOs—more easily accommodate gradations of security levels. This means there is a need to be able to more effectively deal with multiple levels of classification and protection of dissemination within the multiple levels of security. The CIE therefore needs to be able to accommodate the management of access privileges, security and performance. This has both collection and dissemination aspects in terms of access to and use of the CIE.

Language continues to be a challenge in the area of operation and there is a need for machine-translation tools to help fill the interpreter/translator gap. As noted, interoperability means not only technical and political compatibility, but also the will and the means to communicate, to cooperate, and to collaborate: in short, sharing a common culture of communication. When systems are not politically, organizationally, or technically interoperable, information becomes "stove-piped" within a single organization and systems cannot easily collaborate.

The CIE needs to be able to accommodate a diversity of users and their organizational cultures and sensitivities and the communications and information systems capabilities and databases they bring to the S&R operations. There is also a need for improved data collections, decision aides, analysis capabilities, and visualization tools that meet the needs of S&R operations. Included is the need for data and information management strategy for S&R operations that can be used to guide collection management, analysis, and database capabilities. M/S tools to support predictive assessment and course of action planning for S&R operations are need as well, including MOEs and MOPs for measuring progress and success of actions. The CIE needs to be scalable in terms of number and diversity of the civil and military users and must be easily and rapidly deployable into the area of operation and able to accommodate the environment—stand alone capabilities including power and O&M support.

"STRAWMAN" ICT APPROACH TO SATISFY NEEDS.

The creation of a collaborative military and civilian computing and communications environment that enhances information and knowledge sharing for all participants in S&R operations is achievable with today's technology. Such a capability would facilitate information dissemination; data collection and analysis support for decision-makers and staffs (military, political, civil agencies, UN, international organizations, international governmental organizations, non-governmental organizations, and indigenous national leaders, local governments, and businesses); provide knowledge, understanding, and

visualization to help decision-makers make rapid, effective decisions (military and non-military); and leverage the collective intellectual capital and technology of the participants to provide a transparent, seamless, and robust capability that accommodates differences in participant capabilities, policies, languages and other factors and facilitates "plug and play" in order to get the right information to the right place, all of the time for those participating in S&R operations.

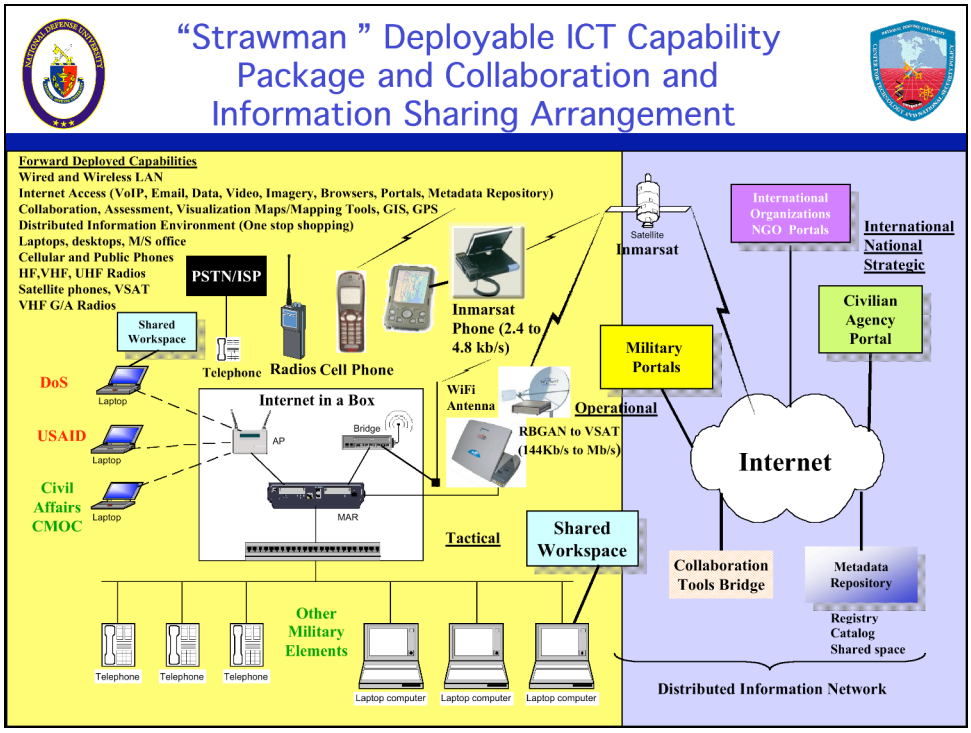


Figure 9: "Strawman" Deployable ICT Capability Package and Collaboration and Information Sharing Arrangement.

The proposed "Strawman" illustrated in Figure 9 consists of several pieces. First, it is assumed that the Internet will be the common link among the civil-military participants and will be used by both the military and civilian elements to communicate and share information. Second, a common suite of ICT capabilities (toolbox) such as cell phones, radios, satellite phones, VSATs, PDAs, laptops, workstations, and applications such as collaboration tools and GIS exist and can be selectively packaged and tailored to meet the anticipated ICT needs for elements responding to a complex emergency. Third, it is assumed that adequate consideration will be given to local regulations governing the use of capabilities such as wireless and large satellite terminals and frequency assignments for radio nets. Proper cell phone configurations are important and it's important to establish service provider agreements with satellite, telecos, ISPs and Teleports before deploying ICT capabilities forward. And forth, both the civilian and military elements will create Internet portals and a metadata repository will be created to provide a one stop shopping capability for access to and knowledge about the complex contingency. Collaboration tool bridges will also exist to facilitate exchange among different collaboration tools.

It is assumed that the community will employ smart systems engineering to create local radio nets to facilitate communications among responders on the ground and that an agreement will exist for data standards and smart management of the information and

knowledge that will populate the various web portals created to support the response operation including the creation of metadata repository to facilitate information discovery. Information assurance will need to be more than "trust" and self-discipline by the user community. The community will need to have agreed mechanisms in place to insure the quality and integrity of information populating the web sites. Finally, appropriate network security protection needs to be implemented to protect against intrusions, viruses and malicious code.

DATA FOR S&R OPERATIONS

As a cautionary tale, it must be emphasized that the data problem is not new. The following quote from Sir Josiah Stamp underscores the fact that extensive processing of data should not obscure its inherent lack of quality or credibility.

> "The government are very keen on amassing statistics. They collect them, add them, raise them to the n-the power, take the cube root and prepare wonderful diagrams. But you must never forget that every one of these figures comes in the first instance from the village watchman, *who just puts down what he damn pleases*."
>
> —Comment of an English judge on the subject of Indian statistics;
> Quoted in Sir Josiah Stamp in "Some Economic Matters in Modern Life"

However, the changing face of conflict is altering the nature of the data problem. In S&R operations, the participants deal with data that are progressively more multi-sectoral (e.g., political, military, health, shelter), multi-dimensional (descriptive of the affected population, vulnerable groups, assistance), contextual (e.g., historical, cultural, ethical), multi-source (e.g., government, International Organizations (IOs), Non-Governmental Organizations (NGOs), media), and non-standardized (e.g., with respect to formats, definitions, indicators, measurement indicators, and methodologies). In addition, they must confront the challenges of data overload while simultaneously redressing data gaps.

Consequently, one of the major problems is synthesizing this mass of heterogeneous data into a form that can readily be digested by the decision maker. That is prompting the community to develop and implement innovative graphical interfaces. As an example, the Humanitarian Information Unit (HIU) in the Department of State is pursuing Visualized Information & Synthesized Temporal Analysis (VISTA).

Given the current operational challenges facing the US Government (with the challenge of transforming Iraq from a failed to a functioning state), it is clear that the data problems cited above are rapidly becoming representative of the data issues that participants in an S&R operation must confront.

Over the course of the last few years, there have been numerous workshops on the subject of data for S&R and humanitarian operations (References 3 and 4). Table1 identifies an incomplete list of the data issues that were identified during those workshops. It is notable that the issues cited are numerous and exceedingly challenging.

• Data sharing	• Data acquisition
• Data conversion	• Data reuse
• Lack of good data dictionaries	• Data bloat
• Lack of knowledge of original purpose	• Data protection
• Data subrogation	• Data naming conventions
• Data purity	• Data maintenance
• Metadata policy (e.g., standardization)	• Data shelf life
• Ontological development for intelligent searches	• Data reconciliation

Table 1: Selected Data Problems Facing the S&R Community

It is widely recognized that there are many barriers to the effective reuse of data. These include, *inter alia,* the lack of knowledge about the existence of legacy data; security or proprietary restrictions; the quality of metadata (e.g., the failure to document conditions of collection); varying definitions, language, and measurement instruments; the form of accessible data; the rapid change of technical data; and the fear that data could be misused, misunderstood, or lead to adverse consequences.

There has been broad agreement at these workshops that the goals of the S&R community can be broadly divided into two macro-objectives. First, it is critical that the data be *available* to the user. To do so, it must be visible, accessible, and institutionalized. In particular, it is essential that these data must be rapidly available if the analyst is to be responsive to the short suspenses mandated by decision makers. Second, the data must be *usable* by the recipient. This implies that it must be understandable, trusted, interoperable, and responsive to user needs (e.g., in the appropriate format).

PROPOSED STRATEGY AND APPROACH

Currently, the NDU in partnership with ASD(NII), is undertaking a data initiative for S&R that systematically employs the DoD Net-Centric Data Strategy (Reference 3), suitably adapted to satisfy the needs of the S&R Community of Interest (COI). In order to implement this concept, there is interest in employing an *evolutionary* approach. This approach is based on four key steps. As a foundation, it is necessary to develop the broad data needs and information exchange requirements for the S&R COI. Second, it is appropriate to formulate an architecture to guide the activity. This would include a characterization of the "as is" situation, the desired "to be" situation, and the path to evolve from the baseline. Third, it is vital to rapidly develop a core capability to satisfy immediate needs. Finally, it is important to commit to the periodic development of increments that reflect feedback from the users, provide additional capabilities and functionalities, and incorporate emerging information technologies. These key steps are depicted schematically in Figure 10.

In the cover letter to the DoD Net-Centric Data Strategy, John Stenbit (then-Chief Information Officer of DoD) identified the four key attributes of the strategy. These consist of the following:

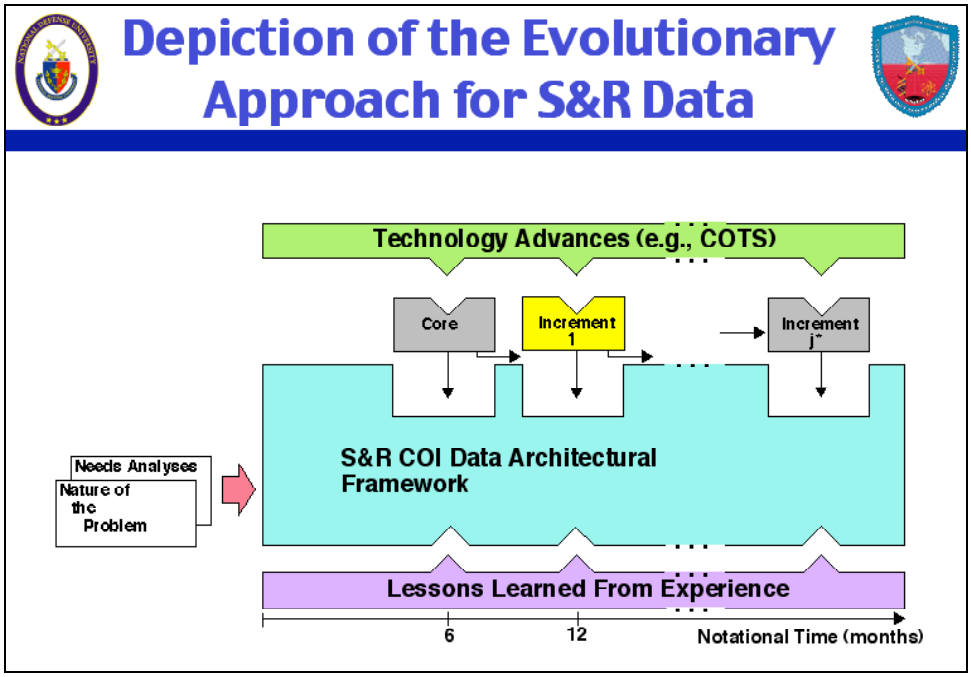


Figure 10: Depiction of the Evolutionary Approach for S&R Data.

- Ensure data are visible, available, and usable when needed and where needed to accelerate decision-making.

- "Tag" all data with metadata to enable discovery of data by users.

- Post all data to shared spaces to provide access to all users except when limited by security, policy, or regulations.

- Advance the COI from defining interoperability through point-to-point interfaces to enabling the "many-to-many" exchanges typical of a net-centric data environment.

The DoD Net-Centric Data Strategy formulated a data vision that was predicated on three key elements:

1. *COIs* to address organization and maintenance of data.

2. *Metadata*, which provides a way to describe data asses and the use of registries, catalogs, and shared spaces, which are mechanisms to store data and information about data.

3. *Global Information Grid (GIG) Services* that enable data tagging, sharing, searching, and retrieving.

The DoD Net-Centric Data Strategy identifies a set of seven goals to make data more readily available and usable. For each of those seven goals they have identified a set of actions to achieve those goals. Although these goals and actions are generic, they can be tailored to meet the needs of the S&R community.

- *The first of these goals is to make data visible*. This is to be achieved by posting data to shared spaces, associating discovery metadata with data assets, creating and maintaining catalogs; registering metadata related to structure and definition, and inventorying data assets.

- *The second goal is to make data accessible*. It is recommended that this be implemented by creating shared spaces and data access services and developing associated security-related metadata.

- *The third goal is to institutionalize data management*. To do so requires that the community govern data processes with sustained leadership; incorporate data approaches into COI processes and practices; advocate, train, and educate in data practices; and adopt metrics and incentives.

- *The fourth goal is to enable data to be understandable*. This can be accomplished by defining appropriate ontologies and metadata. The latter should subsume both content- and format-related metadata.

- *The fifth goal is to enable data to be trusted*. To approach this issue, it is necessary to associate data pedigree and security metadata, and to identify authoritative sources.

- *The sixth goal is to support data interoperability*. A set of four steps are envisioned to realize that goal. These include registering metadata, associating format-related metadata, identifying key interfaces between systems, and complying with net-centric interface standards.

- *The final goal is to be responsive to user needs*. This implies involving users in COIs and establishing a process to enable user feedback.

WAY AHEAD

This paper briefly summarized the insights that have been developed for ICT systems and data in support of S&R operations. It is observed that the civilian and military elements participating in S&R operations need to communicate, collaborate and share information but factors such as civil-military organizations and people cultural differences, language differences, restrictive military security procedures and International Organizations (IO) and Non-Governmental Organizations (NGO) impartiality sensitivities and unwillingness to deal directly with military elements challenge the degree to which collaboration and information sharing is achievable on the S&R ops landscape.

Further complicating the situation is the fact that the participants, especially the civilian elements, deploy with a varying degree of information communications technology (ICT) capabilities that can range from nothing but a pencil and paper to sophisticated systems. The ICT capabilities deployed are independent and tailored (often minimum capabilities) to try to meet anticipated mission needs of the participants with little to no attempt to build a federated network through a more informed and smart interconnection of the stove-piped systems to gain economies of scale and improve the operational coverage and capacity

serving the participants on the ground and their supporting organizations as well as the local population and leadership they are trying to help.

Additionally, the S&R data problem is complex and enormous and increasing in both complexity and size! Recent workshops have served to showcase several significant initial steps that the community has taken to address the problem. These include the efforts of NDU, ASD(NII), and the Department of State to develop a common understanding of the problem, initiate key actions to address the most significant shortfalls and develop an "ICT Support to S&R Ops Primer.".

ESTABLISHING A CIE

Commercial ICT solutions exist to rapidly extend communications connectivity and capacity and information services into S&R areas of operation to facilitate communication and collaboration. The Internet has become the de facto civil-military collaboration environment in support of S&R Ops and both civilian and military elements employ Internet portals to create a distributed information environment to facilitate information sharing but the systems and data management of this ad hoc environment remains a challenge. Some steps to improve the situation include:

- Conduct an assessment of information needs and existing knowledge resources in advance, and identify the gaps in data, information and knowledge.

- Provide standardized meta-data (source, date, geo-reference, definitions) along with all collected and shared information, so that it can be pooled, compared, verified, mapped, and used for analysis.

- Establish and use collaboration networks to create communities of interest among individuals in multiple organizations as a means to capture and share tacit knowledge and dismantle organizational stovepipes.

- Employ visualization to represent complex data and information, display patterns and relationships, and depict a geo-spatial common operating picture.

- Demonstrate the practical applications of new information tools and technologies and use collected data and information to answer questions and respond to identified information needs.

- Recognize the value of tacit knowledge gained from field experience, collaboration and learned expertise.

- Promote the use of new tools and technologies, such as Personal Digital Assistants (PDAs), Global Positioning Systems (GPS), Geographic Information Systems (GIS), and virtual collaboration networks and provide advance training in order to ensure that personnel use them effectively and routinely in their work.

- Create an environment of willingness to conduct more open sharing between the civilian and military participants

- Seek achievement of an agreed strategy, CONOPS, systems architecture and standards for ICT support to S&R ops

- Develop an ICT technology roadmap—near, mid and long term.

  > ICT capabilities (cellular, satellite phones, VSAT, wireless networks, PDAs).

  > Collaboration and information sharing (peer to peer, web pages, portals, GIS).

  > VoIP

  > Metadata repository (registry, catalog, shared workspace)

- Seek agreement on organization arrangements for creating and maintaining a civil-military collaborative information environment that supports S&R ops, including managing the distributed information environment and system of systems supporting this environment

- Develop an ICT support to S&R Ops Primer.

  > Shared understandings of participants roles, relationships and capabilities.

  > Principles for Information and Information Exchange Requirements.

  > Tool kits and fly away package options.

  > Best practices.

- Develop and acquire ICT fly away packages for use by civilian government and military participants that facilitate collaboration and information sharing with IOs and NGOs and can be used as leave behind ICT starter packages for building host nation capacity

BEST PRACTICES—A START

Based on prior workshops on data for S&R and humanitarian operations, a strawman set of best practices has been developed. The following section briefly summarizes those best practices. It must be emphasized that this set is still incomplete and it remains to develop an extended, validated set of "necessary and sufficient" best practices. The strawman best practices can be broadly divided into those associated with guidelines for civil-military coordination, preparing for an S&R operation and those associated with conducting the operation.

GUIDELINES FOR CIVIL-MILITARY COORDINATION AND INFORMATION SHARING

- Understand the other actors
- Respect legitimate limitations
- Pay special attention to geographic and sectoral boundaries
- Leverage the shared interests of actors
- Build and carefully use networks
- Take the initiative in information sharing
- Have multiple simple reliable means of sharing information
- Encourage training and preparation for task sharing
- Provide the tools to facilitate joint planning
- Avoid public criticism of any actors
- What are the commander's orders or policies regarding the sharing of information with civilian humanitarian organizations?
- What are the existing channels for communication between humanitarians and military forces at various levels and how do they work in emergencies?
- Does anyone in the humanitarian community have access to the operations centers or command posts?
- What role does the Civil Military Cooperation (CIMIC) Officer and the Civil Military Operations Center play in sharing information with humanitarian actors?
- Is the communication and exchange of information dependent on translation?
- Are military officers reluctant to share information in the presence of or with local humanitarian staff?
- What are the informal and technical channels for the exchange of information between the humanitarians and the military force?
- What mechanisms are used by the military force to provide information to the population and are these sources trusted by the population?

- Has a Humanitarian Information Center (HIC) or similar facility been established and does the military force receive or provide information from or to this facility?

- Have any of the agencies or the Humanitarian Coordinator placed restrictions on the information that can be shared with military organizations?

- What is the primary means of sharing information among agencies and other humanitarian that has been received from a military force?

- Are there established procedures for safeguarding sensitive information such as "UN Restricted" communications or documents?

- Has a formal process been established for requesting information from military forces and is there effective follow-up on requests?

- Do any of the major actors in the humanitarian community feel they have been unnecessarily denied information or deceived by the military force?

PREPARING FOR AN S&R OPERATION

- S&R organizations need to establish strategies and systems for the management of data, information, and knowledge. These functions need to be planned for, resourced, and set up prior to an operation and prior training for these functions and systems is required.

- Short, simple, standardized templates are needed to facilitate the collection and rapid assessment of data. However, advance training and organizational commitment are critical. In addition, these templates must be "socialized" among other members of the S&R community so that they are consistent and mutually supportive.

- Technology is not the limiting factor with respect to data. However, new technologies (e.g., PDAs, GPS, virtual collaboration tools) require advance training in order to be effective.

CONDUCTING THE S&R OPERATIONS

- Know how to get in contact with the right people in the most expeditious and appropriate manner to facilitate resolution of civil military issues.

- Since no single organization has all of the data, information, and knowledge about S&R, sharing of information is essential.

- Within the USG, almost all of the data and information about complex emergencies come from open source or unclassified sources. However,

Defense and Intelligence agencies often disseminate their information using classified platforms and channels. As a best practice, if it is appropriate, they should use unclassified, open sourced platforms and channels for this unclassified information.

- A formal process needs to be established for the humanitarian community to request information from the military forces.

- There is an overall need for a common operational picture and enhanced situational awareness. This calls for the creation of a common relevant, releasable operational picture that can be used by all.

- Information should be collected, organized, and disseminated in a manner that will benefit the population and polity of the affected host country.

- Standard Map Sheet, Coordinate System, and Location Names: The military will work from a standard map or map series and a common coordinate system. The same is not true of the humanitarian community, especially the NGOs. Most military organizations use the Universal Transverse Mercator (UTM) grid system and maps in common sizes such as 1:25,000, 1:50,000 and 1:250,000. Most commercial GPS work in longitude and latitude. In some cases sophisticated GIS systems will translate between these systems, however, the most reliable means is to have a transparent overlay with the alternative grid system for the military map and the most common humanitarian maps.

- Consolidated and maintain a list of place names with alternative versions in the native languages and variants in spelling because most incident information received from local sources will reference neither the military or civil grid system.

- Frequency and Bandwidth Management: Control of the use of the electro-magnetic spectrum is the responsibility of the government in each state. Specific frequencies are reserved for specific activities. Important frequencies for international communication, such as air traffic control, are established by international treaty. Other frequencies such as those used for commercial radio transmission are controlled by the government and licensed. In the absence of an effective governmental agency to deal with the monitoring and enforcement of these matters, the international military and civilian communications specialist must come to an agreement on these matters or communications can be severely disrupted, especially in emergencies where radio discipline may be weak.

- More sophisticated military forces and IOs will often buy satellite access from commercial satellite providers to supplement their own satellite systems. This can dramatically increase the price of access or limit availability for humanitarian actors. At a minimum, a memorandum of understanding should be negotiated to ensure equitable access to both frequencies and satellite resources.

In order to make additional substantive improvements in data support to S&R ops, it is vital that the civilian and military community take several challenging steps. The most of important of these steps is an initiative to transform the culture of data from one of hoarding to one of sharing. To do so, steps must be taken to dispel the fears that permeate the community (e.g., fears of misuse, misunderstanding, and adverse consequences). This initiative must be undertaken and sustained at the highest levels of leadership among the civilian and military participants. Second, the "people" issues must be addressed. This entails educating and training the users and providers of data -- and the decision makers! Finally, if there is one key technical issue to be worked it is that of metadata. The participants at the workshops have highlighted this theme over and over again. The problem is challenging and the community must begin to address it seriously and immediately.

REFERENCES

1. USIP, 2004. "Creating a Common Communications Culture", Virtual Diplomacy Initiative, USIP.
2. Johnson, Stuart, 2004. "Transforming for Stabilization and Reconstruction Operations", Hans Binnendijk and National Defense University.
3. Orr, Robert C., (ed.) 2004. "Winning the Peace: An American Strategy for Post-Conflict Reconstruction.' Washington, D. C.: The CSIS Press.
4. "DoD Net-Centric Data Strategy", ASD NII, May 9, 2003.
5. "Multilateral Interoperability Programme: The C2 Information Exchange Data Model," Greding, Germany, October 1, 2004.
6. UN OCHA Civil-Military Coordination training material, 2005
7. DoD Instruction 8110.1, Multinational Information Sharing Networks Implementation, 6 February 2004.
8. Lidy, Martin, 2005. Miscellaneous S&R related briefing material, IDA.
9. King, Dennis, 2005. " Humanitarian Knowledge Management", U.S. Department of State, Humanitarian Information Unit, ISCRAM Conference, April 2005.