Information and Information Communications Technology as an Enabler of Success in Stability and Reconstruction Operations

Larry Wentz

Center for Technology and National Security Policy
National Defense University
Fort Lesley J. McNair, Washington, D.C., U.S.A.
e-mail: Wentzl@ndu.edu

Larry Wentz is a Senior Research Fellow at the National Defense University Center for Technology and National Security Policy. He is an experienced manager, strategic planner, C4ISR systems engineer, author, and lecturer. In 2006 he visited Afghanistan to research Afghanistan Telecom and IT reconstruction and documented his findings in the NDU report titled, ICT for Reconstruction and Development: Afghanistan Challenges and Opportunities. While on special assignments to ASD (C3I) Command and Control Research Program (CCRP) he authored two NDU/CCRP published books: Lessons from Bosnia: The IFOR Experience and Lessons from Kosovo: The KFOR Experience. Mr. Wentz was a Research Scientist at the George Mason University Center of Excellence in C3I, a Vice President of Advanced Communication Systems-Washington Operations and Technical Director at the MITRE Corporation. He received a B.S. in Electrical Engineering from Monmouth College and a M.S. in Systems Engineering and Operations Research from the University of Pennsylvania. He completed the Executive Management Program at the University of Pennsylvania's Wharton Business School and the Harvard John F. Kennedy School of Government Program for Senior Executives in National and International Security.

ABSTRACT

Information and information communications technology (I/ICT) can significantly increase the likelihood of success in stability and reconstruction operations—*if* they are engaged as part of an overall strategy that coordinates the actions of outside intervenors and focuses on generating effective results for the host nation. Properly utilized, I/ICT can help create a knowledgeable intervention, organize complex activities, and integrate stability and reconstruction operations with the host nation, making the latter more effective.

Key to these results is a strategy that requires that (1) the U.S. Government must give high priority to such an approach and ensure that the effort is a joint civilian-military activity; (2) the military makes I/ICT part of the planning and execution of the stability operation; (3) preplanning and the establishment of I/ICT partnerships is undertaken with key regular participants in stability and reconstruction operations, such as the United Nations (UN) and the World Bank; (4) the focus of the intervention, including the use of I/ICT, is on the host nation, supporting host-nation governmental, societal, and economic development; and (5) key information technology capabilities are harnessed to support the strategy. Implementing the strategy will include 1) development of an information business plan for the host nation

so that I/ICT is effectively used to support stabilization and reconstruction; 2) agreements among intervenors on data-sharing and collaboration, including data-sharing on a differentiated basis, and 3) use of commercial IT tools and data provided on an unclassified basis.

The thoughts discussed herein are based on research work done at the National Defense University Center for Technology and National Security Policy and in particular, an effort referred to as I-Power.[1]

BACKGROUND

Over the past 30 years, the information revolution has had an important impact on the conduct of military operations. In the United States, it has produced what is often called "netcentric warfare" or "netcentric operations"[2]—the combination of shared communications, key data, analytic capabilities, and people schooled in using those capacities—that has enabled enhanced joint activities, integrated distributed capabilities, much greater speed, and more effective maneuver. The result has been that the United States and its allies have been able to conduct very effective combat operations under a range of conditions, including quick insertion (Panama), maneuver warfare (major combat operations in Iraq), an all-air campaign (Kosovo), and a Special Forces-led effort (Afghanistan).

At the same time that major combat operations have proceeded so successfully, the United States and its allies have undertaken a variety of stability operations in Somalia, Haiti, Bosnia, Kosovo, East Timor, several African countries, Afghanistan, and Iraq.[3] These stability operations generally have included both economic and governance reconstruction and have spanned the full security gamut from nonviolent peacekeeping to full-blown counterinsurgency. Not one of these operations has approached the success achieved in combat operations undertaken in the same period.

This paper analyzes whether a strategic use of information and information communications technology (I/ICT) in stability operations could lead to more successful operations. Certainly, the information revolution has been a dynamic and positive factor in business, government, and social arenas in the Western world. The combination of technology, information content, and people schooled in the use of each has reshaped enterprises and activities of all types. This paper concludes that utilizing the elements of the information revolution in a strategic approach to stability and reconstruction operations would have positive results and sets forth the strategic and operational parameters of such an effort.

STABILITY AND RECONSTRUCTION OPERATIONS CHALLENGES

Utilizing the fruits of the information revolution for effective stability and reconstruction operations requires a prior understanding of what makes these operations effective. As noted above, stability operations have security, economic, and governance reconstruction elements. Yet while it is widely recognized that stability operations go far beyond purely military actions—encompassing security, humanitarian, economic, and governance/rule of law issues

—no one has set forth an actual strategic or operational doctrine that promises success in stability and reconstruction operations. As a World Bank staff report put it, "The Bank, like other international partners, is still learning what works in fragile states contexts."[4]

The challenges of stability and reconstruction operations are evident. To begin with, no two circumstances are the same. To say that Haiti is different than Somalia is different than Bosnia is different than Afghanistan is only to hint at the depth and breadth of the complexities. These include the causes of the crisis that occasioned the intervention, the host-nation culture or cultures, the language or languages, the nature of the economies *ante bellum*, the influence of neighbors, and a multitude of other factors. By definition, the state structure has collapsed or is severely impaired. Often there has been significant violence. Internal groups have been factionalized and frequently have each others' blood on their hands. Economies are in disarray. Social mechanisms have broken down. Information is lacking, and communications mechanisms are limited.

ICT activities supporting stabilization and reconstruction operations in an affected nation can be problematic as well. These activities suffer from a lack of adequate understanding of the affected-nation information culture and ICT business culture. No agreed architecture or plan is in place for affected-nation ICT reconstruction. There is no clear mapping of responding stakeholder organizations roles and responsibilities. Program development, project coordination, information sharing, and ICT implementation are largely uncoordinated and non-standard. Few formal mechanisms are in place to create a collaborative information environment to facilitate cooperation, coordination and information sharing and to help de-conflict and leverage ICT investments.

Additionally, there is little doubt that ICTs are an engine for social and economic development but quantifying their impact is difficult. Evidence remains largely anecdotal, and the link between ICT deployment and reconstruction and development remains vague. The absence of designating ICT as an "essential service" further contributes to the challenges and a general lack of visibility of ICT initiatives and coordinated investment strategies—no shared situation awareness for ICT initiatives, a lack of ICT metrics for measuring impact and progress and a general lack of awareness of who is doing what, where, when, why and for how much in the ICT sector and ICT support to enable other sectors.

Prior to almost all interventions, the international community will already have been significantly present in the form of international organizations, nongovernmental organizations, businesses, bilateral governmental activities, and many more venues. Once there is a major international intervention, complexity increases greatly. Regardless of the initial number of international actors, the number and diversity of participants increase. More importantly, their relative importance increases for such functionality as exists or is created in the host country. Additionally, whereas before the intervention, development often had priority, now there are simultaneous challenges in the security, humanitarian, economic, and governance arenas—and, if social needs may be separated from the foregoing, in the social arena as well. Because of the expanded requirements, there are numerous players. Personnel and equipment stream in from civilian and military components of the governments of the United States and other nations, international organizations, such as the United Nations (UN) and its many agencies, the North Atlantic Treaty Organization (NATO), the Organization for Security and Co-operation in Europe, the African Union, the World Bank, and others. Nongovernmental organizations also are involved, many of them in the humanitarian arena, as well as numerous others that participate in myriad aspects of reconstruction and

development. Many businesses also get involved, either as contractors to national and international organizations or as participants in private ventures.

A very important aspect of the complexity is that dealing with the host nation has become more difficult. Governmental functions are broken, and the government is seen by many as illegitimate and not representative of all the people; its reach is generally limited, and it is ineffective in mobilizing domestic human and other resources.

A further complicating factor is that circumstances on the ground change over time in significant part in response to the intervention. (The transformation from liberator to occupier is a well-known problem for intervening forces.) Interventions generally last for years, and a decade is not unusual. Stability operations encompass not only security but also reconstruction, and reconstruction takes time. In addition to actual changes, managing expectations of both the intervenors and the host nation becomes extremely important. For example, there is a so-called "golden hour" of 6–12 months during which actions must support expectations and the local population must experience improvements in quality of life.

It is in this context that the question arises whether the application of the tools and content of the information revolution can have a positive effect on the outcome of stability and reconstruction operations.

OPPORTUNITIES FOR AN INFORMATION AND ICT STRATEGY

As difficult as the circumstances of stability and reconstruction operations are, the very complexity provides significant opportunities for the use of an effective information strategy built around the use of information technology. It is worth underscoring at the outset what may be an obvious proposition: that information and information communications technology have to be used together to be effective. One will not suffice without the other.

At the most basic level, information communications technology can be used to distribute information to important players in an ongoing stability and reconstruction operation. Making information available can have four important consequences.

First, it can *help create a "knowledgeable" intervention*. Even before the intervention, and certainly as the intervention progresses, the intervenors will need information of many kinds about both planned and ongoing respondent activities and about the host nation. For the latter, population characteristics, cultural dynamics, economic structures, and historical governance issues all can be described and analyzed.

The intervenors will first plan and then undertake many activities, with multiple players in each field of endeavor. While it will not be possible for all intervening actors to have the unity of command that is sought by militaries, the use of I/ICT may allow for organizing a more common approach—or at least to reduce inconsistent approaches.

An information strategy supported by information communications technology provides an opportunity to share information among the stability operation respondents themselves. This sharing of information will facilitate the generation of a common approach and can help

in the effective use of scarce resources. As an example, the allocation of health care resources might be usefully rationalized once there is at least a working sense of what types of resources are available from the respondents. Also, intervenors working on the rule of law in different sections of the country will be more effective if they adopt closely aligned approaches than if they use significantly different approaches, even if each is valid in and of itself.

A second key element of the strategy will be using I/ICT to *help organize complex activities*. Normally, a stability operation will be undertaken on a country-wide basis. For even the smallest countries, this means a significant geographic arena, with all the difficulties of maintaining connectivity. The intervention also will undoubtedly extend over a significant timeframe, and I/ICT will be necessary to maintain an updated approach as conditions on the ground change.

Complexity also will be manifested in the requirement to deal simultaneously with security, humanitarian, economic, and governance issues. Many intervenors will be involved in only one or some of these actions, but actions in one field often have consequences for another. Moreover, knowledge of what is happening in each is important for the development of an overall strategy capable of achieving an effective host nation. Even in a single sector, information supported by effective information communications technology would allow for more effective in-country coordination; and distributed players would be better able to take focused effective actions. Furthermore, knowledge is an important element in building trust and commitment among different stability and reconstruction operations players, which can be a key element in enhancing effectiveness.

The third key use of distributed information will be to *integrate the stability and reconstruction operations respondents with the host nation*. It bears stating more than once that the objective of a stability and reconstruction operations is not a "good intervention" but rather an "effective host nation" as a result of the intervention. To accomplish this difficult task, given that the host nation is likely fragmented, disrupted, and not very effective, the intervenors need to stay connected to the host nation so that the results are adopted and adoptable by the populace on whose behalf the effort is being undertaken. An I/ICT strategy needs to involve the host nation (likely in numerous manifestations) in the ongoing activities of the intervention.

The fourth use of I/ICT is to *integrate the host nation and make it more effective.* Effectiveness can be enhanced by using I/ICT to identify key requirements and target scarce resources. Information for a budget process is an important example. I/ICT will also be able to facilitate informed senior decision-making well beyond budget and budget-type decisions. For example, how best to bring previous warring factions to work together will involve important social and economic issues whose resolution can be enhanced by good information.

Host-nation capacity can also be created by the use of I/ICT. Government operations can be reestablished with the proper use of information communications technology. Both the information systems and the training to use them will be required, but information capacity can be generated far more quickly than other infrastructures—and can enable other effective actions.

KEY QUESTIONS FOR THE I/ICT STRATEGY

An important question in analyzing an I/ICT strategy for stability and reconstruction operations is how such a strategy relates to what else is happening in the intervention. As noted by the World Bank staff, no one has developed a truly knowledgeable approach to stability operations, which, in World Bank parlance, is one type of activity in fragile states. There are, however, some principles that have been adopted by the international community and the United States that are worth noting here.

First, the international community, through the Organisation for Economic Co-operation and Development (OECD) and otherwise, has emphasized the importance of the principles of harmonization and alignment. *Harmonization* refers to having the outside intervenors work in a generally coordinated fashion. As the OECD Development Co-operation Directorate has stated, "Harmonisation is taken to refer to common arrangements amongst the donor community, rationalized procedures and information sharing between donors . . . related to the goal of greater coherence between and among donors."[5] *Alignment* refers to having the outside intervenors align their activities with the interests of the host nation. Again, as the OECD Development Co-operation Directorate stated, "Alignment has been defined . . . as a set of practices according to which donor organizations use recipient country strategies, policies, and practices . . . as a guide for their assistance programs."[6] Both these principles are embodied in the so-called Rome Declaration on Harmonization of 2003 and subsequent actions and statements of the major multilateral and bilateral donor entities and countries, including the United States.

I/ICT can have an important, positive impact on both harmonization and alignment. Coordination among intervenors is one of the key achievable results of an effective information strategy implemented by information communications technology. Likewise, an I/ICT strategy is an important element to ensure that the host nation is effectively integrated into the decisionmaking and implementing actions of the outside intervenors.

A second question is the relationship between an I/ICT strategy and strategies for security, humanitarian needs, economic development, and governance/rule of law. The U.S. Government, and particularly the Department of Defense (DOD), has often talked about using all elements of national power for success in stability and reconstruction operations, often citing diplomatic, informational, military, and economic (DIME) power as key aspects of the types of power brought to bear by outside intervenors.

This so-called DIME paradigm is a useful model, although it is not meant to be exhaustive. For example, host-nation civil society may be affected by outside, nongovernmental, civil organizations that nonetheless are important elements of an intervenor's national power. Social issues also must be considered, and, unless "diplomatic" is read to mean all contacts other than military or economic, there will be important nondiplomatic interactions on matters such as rule of law. What the DIME paradigm shows most importantly, however, is that information needs to be considered in an overall context, just as the principles of harmonization and alignment indicate.

There is a sterile debate as to whether information only supports other activities or is an activity in and of itself. Certainly, information supports other activities. Military, economic, and governance activities all operate on the basis of information. Conversely, certain aspects

of information, such as the establishment of technical structures, can be undertaken apart from other activities. As an example, think of the building of towers to create the infrastructure for a cellular network. Overall, however, information, as every other action in a stability and reconstruction operations, is designed for one purpose: to serve the objective of making the host nation effective. That is the overall context in which to consider I/ICT and to determine whether and how to undertake a particular effort.

The broad challenge for an I/ICT strategy for stability and reconstruction operations is to help create effective results from the multitude of players and actions that will be found in a particular situation. No one should think that information is a panacea. If a faction within a country resists working with another faction even after all information is exchanged, then that is a political problem and probably will not be solved by further information. But given that information is not a universal solution to all problems, the question is whether the information revolution can help harmonize, align, and make more effective the outside military and civilian governmental intervenors, international and nongovernmental organizations, businesses, and, especially, host nation in all its manifestations.

ELEMENTS OF AN I/ICT STRATEGY

ELEMENT 1 OF AN I/ICT STRATEGY

Five key elements are required to generate an effective I/ICT strategy for the United States to use in stability and reconstruction operations. The first requirement is for the U.S. Government to make the fundamental decision that such a strategy is a key mandatory element of all stability and reconstruction operations. That is no small statement, because the reality is that the United States has never—in any of its many stability operations—made such a decision. But the rationale for such a conclusion is clear: information and information communications technology are crucial elements to the success of stability and reconstruction operations, supporting effectiveness, harmonization, and alignment goals.[7]

A coherent U. S. Government I/ICT strategy is essential to produce the needed results. This means that the effort has to be truly interagency—and, most importantly, be accepted as a key element by both DOD and the State Department (including USAID). While some individuals have acknowledged this point, no such government-wide I/ICT strategy exists, although a potential framework for one has been created.

Released by the President in December 2005, NSPD-44, "Management of Interagency Efforts Concerning Reconstruction and Stabilization," articulates the basic framework for interagency cooperation. It assigns primary responsibility for stabilization and reconstruction operations to the Secretary of State (through the Office of the Coordinator for Stabilization and Reconstruction) and mandates close coordination with DOD to integrate stabilization and reconstruction contingency planning with military planning, when relevant and appropriate. The Director of Foreign Assistance, who reports directly to the Secretary of State, also serves as the Administrator of USAID, where several offices have been created or restructured to deal with stabilization and reconstruction challenges.[8]

At DOD, the framework was supported in November 2005 by the release of Directive 3000.05, "Military Support for Stability, Security, Transition and Reconstruction Operations," which affirms that such activities represent a core DOD mission and are given a priority comparable to combat operations. It also ensures *effective information exchange and communications* among the *DoD components, US Departments and Agencies, foreign governments and security forces, IOs, NGOs, and members of the Private Sector* (para 5.7.1).

Within this framework, however, the focus on I/ICT has been limited. USAID, recognizing the potential of I/ICT in stability and reconstruction operations, has taken some steps to include I/ICT as a sector and development tool. USAID strategy states that it seeks to leverage I/ICT in conflict management and mitigation missions and in humanitarian assistance operations. USAID also seeks to promote global access to ICT and to assist development through several on-going projects such as the Leland Initiative for Africa, the Digital Freedom Initiative, and the Administrator's Last Mile Initiative.[9]

Since the issuance of DoDD 3000.05, DoD has also taken some ICT-related steps. Prior to November 2006, DODD 2205.02 *Humanitarian Civic Assistance Activities* was interpreted to read that provision of ICT capacity was not an authorized activity in Security, Stability, Transition, and Reconstruction (SSTR) or Humanitarian Assistance/Disaster Relief (HA/DR) operations. Congress provided language in the conference report of the Defense authorization bill that clarified the issue: *"Rudimentary construction and repair of public facilities, under section 401(e)(4) of title 10, United States Code, includes information and communications technology as necessary to provide basic information and communications services."* This now affords Combatant Commanders around the world an opportunity to provide a basic ICT capacity during intervention and leave it behind.

Some important embassies have also taken I/ICT steps. The U.S. Embassy in Afghanistan, within the Afghan Reconstruction Group activity, created the position of Senior Telecom Advisor (STA) to facilitate coordination among both military and civilian U.S. Government elements in country. In Iraq, DOD established the Iraq Reconstruction Management Office within the Embassy structure, and it, too, has a senior telecommunication advisor to unify I/ICT efforts. These efforts are the beginning of a coherent U.S. Government approach to I/ICT. A complete strategy would, however, require the Department of State/USAID to make I/ICT a key element of strategy in stability and reconstruction operations, e.g., designate ICT as an "essential service" and develop USG strategies and plans that support host-nation ICT recovery as well as its use an enabler of cross-sector reconstruction. Creation of STA positions are a good start, but are not an integrated strategy. They do, however, provide a basis to build on.

Unfortunately, good initiatives, if not institutionalized, have downside risks associated with sustaining operational capabilities. For example, with the early 2008 departure of the Iraq STA, these responsibilities and functions are being folded into the US Embassy Economic (ECON) section and at the end of 2008 the same will likely happen in Afghanistan with the termination of the Afghan Reconstruction Group activity at the US Embassy in Kabul. These actions will certainly impact the effectiveness of US Government (USG) support to host-nation ICT. For example, the US Embassy ECON section addresses more than ICT, generally will lack ICT subject matter expertise, ICT is not likely to be a high priority activity, and to further exacerbate the problem, the ECON section tends to be under staffed. Hence, these actions will no doubt result in a further reduction in the ability to

engage and affect host-nation ICT outcomes. Given ICT is an engine for not only short term but more importantly longer term economic and social recovery in failed states, the USG elements that focus on ICT initiatives need to seriously question the reasonableness of these decisions and assess not only 1st order impacts but 2nd and 3rd order effects as well and carefully factor these aspects into future decisions.

ELEMENT 2 OF AN I/ICT STRATEGY

Although the problems of stability and reconstruction operations go far beyond military, the second element of an effective I/ICT strategy recognizes that, doctrinally, the military requires an I/ICT strategy as part of the planning and execution of any stability and reconstruction operations. Accordingly, in both joint and Service documents—plans and the rules and guidance for the development and execution of plans—an I/ICT strategy is a required element.

As noted above, this approach is fully consistent with the military analysis of the DIME paradigm. The key point here is that military planners and operators need to include an I/ICT strategy in their approaches. A subsidiary—but crucial—point is that an I/ICT strategy is *not* a traditional function of the J-6 (the technical information officer on a military staff, the chief information officer in business terms). Rather, I/ICT has to be a function of both J-3 and J-5: that is, built into plans and implementation and policy. The J-6 will be in a supporting and implementing role to help execute the strategy. There is no reason why the J-6 cannot help develop the I/ICT strategy, but it cannot be developed apart from the policy, plans, and execution of the larger effort. This is not a technical problem; it is a strategic effectiveness problem to accomplish host-nation harmonization, alignment, and effectiveness.

The U.S. military has already taken some important steps in terms of using I/ICT as part of a stability operation. Warfighting information technology is available if and when military operations are a required part of the stability operation. This paper does not deal with those issues and instead focuses on the issue of joint stability and reconstruction operations activity writ large—that is, joint within the U.S. Government and combined with other non-U.S. partners. On the latter, DOD has undertaken some very worthwhile efforts under the Combined Enterprise Regional Information Exchange System (CENTRIXS) program[10] to facilitate information sharing among largely coalition military elements and some other USG elements such as DoS.

CENTRIXS is a Web-based network, developed with both commercial off-the-shelf and government off-the-shelf tools. It is designed to provide information among coalition partners in activities in which the U.S. military is involved. For example, U.S. Central Command uses CENTRIXS to support coalition military coordination and information-sharing for the Multinational Force in Iraq and the International Security Assistance Force in Afghanistan. CENTRIXS operates on military classified networks, so it is not broadly available to all participants in a stability operation. It is, however, quite useful for information exchange among coalition militaries and is a good step in the direction of using information in stability operations.

ELEMENT 3 OF AN I/ICT STRATEGY

The third element of an I/ICT strategy for the U.S. Government for stability and reconstruction operations is to pre-establish I/ICT partnerships with key stability and reconstruction operations participants. It is important to underscore the word *key*. It is not possible, and would not be effective, to try to establish pre-existing partnerships with all of the many players who will be involved in stability and reconstruction operations. But there are some very key players from the government perspective.

A few countries can be expected to participate in many and even most operations that the United States does. The United Kingdom is one; Canada and Australia are others. Certain key international organizations likewise will be there. The UN certainly would be involved—though dealing with the UN requires dealing with a variety of UN groups and agencies, since it does not act as a single entity. Thus, planning will be important with the Office for the Coordinator of Humanitarian Affairs, the UN Development Program, the UN Department of Peacekeeping Operations, and perhaps the UN Children's Fund. World Bank is another. NATO is often a player, as well as the European Union. Major nongovernmental organizations will also regularly be engaged in stability and reconstruction operations. In fact, these organizations will generally be there in advance of the U.S. military. The fact that preplanning only includes some players is meant to allow for creation of a useful framework. An effective I/ICT strategy will include many others, and there may be conferences, meetings, and workshops of a broader nature. But real planning will be enhanced by a more limited approach.

ELEMENT 4 OF AN I/ICT STRATEGY

The fourth element of an effective information strategy is to focus on the host or affected nation. The importance of establishing host-nation effectiveness has already been emphasized. Informing host-nation decision-making, enhancing governmental capacities, and supporting societal and economic development are all crucial elements of an information strategy. Working with I/ICT as discussed below can help generate important progress in security, humanitarian, economic, and governance/rule of law arenas. The recognition by the international community of the harmonization and alignment goals is important. However, when information technology is considered, all too often harmonization with respect to the intervenors becomes emphasized as compared to alignment and effectiveness of the host nation. This is backwards. An effective I/ICT strategy is one that makes the host nation effective. Nothing else will do. Thus, a critical element of the strategy is an I/ICT business plan for the host nation and an intervenor support strategy that aims to enable the host-nation business plan.

ELEMENT 5 OF AN I/ICT STRATEGY

The last element of an I/ICT strategy will be to work with others to use the key technical capabilities to support the effectiveness, harmonization, and alignment goals. The specifics are discussed below, but a crucial point is that generating the technical part is far less about

invention—the information revolution has given us and continues to give us broad capabilities—than it is about developing ways to use those brilliant inventions in an overall effective, collaborative fashion. The planning aspects of the strategy are crucial to effective use of the tools. Common choice can create highly effective capabilities. Divergent choices can undercut well-meaning strategies.

OPERATIONALIZING THE I/ICT STRATEGY

It is one thing to have a strategy; it is quite another to implement it effectively. The discussion below sets forth how to implement an operational I/ICT strategy. A key point is to remember that both the end goal (creating an effective host nation) and the strategic context (the I/ICT strategy itself) must be developed and implemented inside an overall approach of harmonization and alignment that supports enabling the host-nation security, humanitarian, economic, and governance activities.

To effectuate those tasks, the U.S. Government needs to adopt an information business model with multiple key elements. Those who have responsibility for the I/ICT strategy, which ideally will be a joint effort led by the Department of State (including USAID) and DOD, will need to run the business model in a focused, long-term fashion; otherwise, achievement of the strategic aims will be jeopardized.

The elements of the business model break down into two broad elements: harmonization among outside intervenors, and effectiveness and alignment for, and with, the host nation.

HARMONIZATION

On the harmonization side, a good place to start operational analysis is to recall the complexity of the problem and the number of intervenors. As discussed above, an important element of the strategy is to undertake preplanning with key partners. There are four important elements of preplanning to achieve harmonization.

First, joint civil-military information planning will be critical. In the first instance, this needs to be done between the Department of State, USAID, and DOD, but most importantly it needs to be done between the U.S. Government and other major intervenors to harmonize their interventions. It is not an impossible task to keep others informed and aware, but it is difficult. Issues arise immediately as to what data can be provided and how information can be exchanged. With respect to the latter, development of agreed management and data standards can fundamentally enhance the provision of information. Pre-event planning and face-to-face meetings can enhance trust and provide important education about others' methods. While the myriad of actual stability operations has provided some reasonable knowledge about different key actors, on-the-job learning is necessarily more difficult because of the requirement to do one's "day job." Accordingly, some common training, exercising, and/or education away from a stability operation can create potentially significant opportunities to enhance harmonization. None of this will occur unless an element of the government, preferably a joint Department of State-DOD element, focuses on the requirement for preplanning.

Second, improved collaboration depends on both better processes and use of available technical means. The process issue is perhaps the most crucial. As noted above, it is important to decide how, with whom, and how much data are shared. There is a general tendency, particularly at DOD, to come at the problem through a classified lens. That is, since DOD is used to treating data as classified, the question is often framed as how such data can be made available. Often, the answer is given in binary terms: information either can be made available or it cannot. This all too often becomes a least common denominator approach because the judgment is made that if the data are not available to some, it cannot be available to any.

A much better approach would be to recognize that, in stability and reconstruction operations, most relevant data are broadly available from other than classified sources—though often not broadly collected. Furthermore, and most importantly, data can be shared on a differentiated basis. For example, information provided to UK or Canadian civilian officials can be differentiated from information provided to World Bank officials, which can be differentiated from information provided to Red Cross officials. Groups that have engaged in preplanning and have built up trust will find it easier to share information than groups that meet only in the circumstances of the stability operation. Differentiation is one key element to enhancing data-sharing—and working differentiation as an effective operational approach will depend on preplanning.

Another important step to improve data-sharing will be better use of technical means. For example, the Internet has become a mechanism for unclassified collaboration and sharing of information among civilian and military elements responding to crisis operations. Furthermore, commercially available collaboration tools such as NetMeeting and WebEx and other tools, such as video teleconferencing and Web-cams, are being used by them on the Internet. Technologies are improving quickly to enhance data-sharing. In the civilian arena, the growth of portals, Web logs (blogs), file-sharing, Wikipedia, MySpace, and similar sites all attest to the possibilities of sharing, if the desire to use the mechanisms is there. These new technologies referred to as Web 2.0 promise to facilitate creativity, collaboration, and sharing among users, add a strong social dimension—web links people, and redefine "online" and "offline" actions. In fact, they create a generational divide: "Digital immigrants", those over 30 and "Digital natives," those under 30. Most importantly, however, Web 2.0 launches a new set of dynamics that apply to organizations in general — and therefore to software: distinction between customers and developers blurred; enhances social capital in the real world—"unity of purpose;" freedom to use, modify, and redistribute a source; permanent beta-version—no final development stage; and finally, "more adaptable to the unexpected."

U.S. Joint Forces Command (USJFCOM) has taken strides to enable the sharing of unclassified information with nontraditional partners. The command has conducted several exercises that explore this challenge and Multinational Experiments 4 and 5 specifically address it. The command is also standing up a nonmilitary domain portal outside its firewall that takes an approach more akin to that of a relief organization—many of which are linked to it—than a military one. The portal (http://harmonieweb.org/) enables people and organizations that are participating in a relief effort to obtain and post information that may be valuable in providing the needed assistance.[11] Many non-DoD organizations already run sites to make information available (for example, the UN-sponsored ReliefWeb). However, the collaborative aspect of these sites is limited.

Additionally, the United States is encouraging the development of an open-source, collaborative arena, tentatively called "the hub," that would use blogging, file-sharing, and Wikipedia-type approaches to create an open space for collaborative sharing. It is not clear as of this writing what the outcome of that effort will be. However, even assuming its success, it seems probable that a combination of both a fully open site (the hub or some variant) and a more directed approach (for example, NATO–UN–World Bank collaborative sharing) might be useful. Remember the point about differentiation: to try to use only one tool or one kind of approach to allow for all types of collaboration is not necessarily the most successful approach. Transferring the CENTRIXS in some modified form for collaboration among key civil-military players while generating a broader open-source approach is likely to be a useful effort.

The third element required to achieve harmonization is the development of an implementation strategy. Whatever the precise mechanism for improved collaboration, it can be fairly confidently stated that improvements will not occur absent a strategy that designates elements within the government to make such improvements happen. At the moment, there are good but separate efforts. The Office of the Secretary of Defense is working on the hub effort. USJFCOM is seeking to support elements of the Department of State and, through experimentation, is developing new civil-military coalition processes for improved collaboration and information-sharing and assessing commercial information technology tools for enabling the processes. The recent DOD directive on stability operations requires development of a collaborative information-sharing mechanism.[12] But there is no overall directed effort—and this key element is crucial. Otherwise, the efforts will be personality-driven and ad hoc. Such approaches are way better than nothing but not likely enough to be effective.

A notional picture of an improved approach to collaboration includes broad agreement on the information needed to be collected and exchanged; standards for collection and exchange; technical mechanisms for each that work together; processes; and some education and training together. Figure 1 is a schematic of the elements of a collaborative information approach for stability operations. It is just a model, but it shows the elements of an approach including organizations and people, procedures, infrastructure, and capabilities.

The final important element of collaboration is the ability to improve data usability. As noted above, it is probably useful to think about data in two broad types of collaborative forums: a more limited network among key partners, and a broader, more open network. In each, capacities for search, aggregation, storage, and retrieval are useful and potentially important. Issues of quality control and information assurance will also arise, as will the issue of dissemination.

Technical improvements in recent years have significantly increased the ability to aggregate different types of data, such as the ability to put written information on photographs and to integrate geographic material with other data. That said, there needs to be some data-management group that will determine for the collaborating activity just what kind of capacities will be created—or allowed. For example, it is possible to add to a photograph the names of the people in the picture, but in certain circumstances, adding names might be very hazardous for the individuals identified. An ongoing data-management effort to create rules and manage the activity will be necessary. There is, of course, a technical aspect to this, but some of the key issues will turn out to be policy issues, so the group will need to engage both technicians and policy-makers.

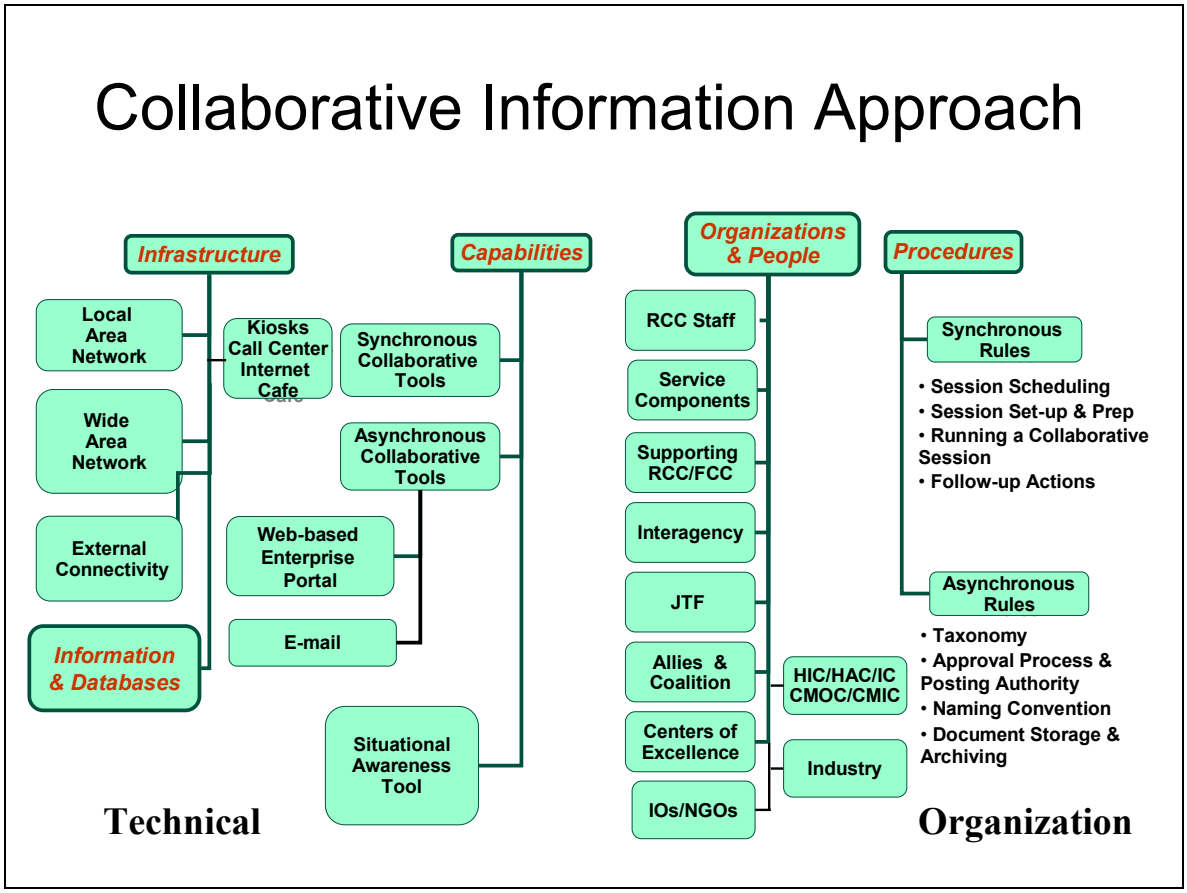

Figure 1: The Collaborative Information Approach.

Information power derives from a combination of people, content, and technical capabilities. In the technical arena, there is a whirlwind of ongoing activity and innovation. A very useful capability would be to have an "information toolbox" that maintains lists of:

- Key information partners, including businesses with technical capabilities;
- Information and data-management tools;
- Other key tools, such as collaboration and translation.

For the effort that we are focusing on here, commercially developed tools are essential because government-generated tools will often not be available to important partners. There will be debates between open-source and proprietary tools, and those debates need to be resolved in actual context, based on what the effort is intended to establish. The case will probably be that the broader the activity, the more desirable the use of open-source—but even that statement needs to be evaluated in the particular circumstance.

The Center for Technology and National Security Policy at the National Defense University has generated a first order "tool kits and best practices" analysis in its recently published *ICT Primer*.[13] That discussion includes, *inter alia*, review of telecommunications capabilities such as satellite communications, creation of a civil-military information environment, data and information management, and best practices. Maintaining and updating such an activity is an important element of an overall strategy.

EFFECTIVENESS AND ALIGNMENT

The fundamental task of an I/ICT strategy is to enhance host-nation capacity. That is the critical result for which the stability operation is undertaken. To accomplish that result in an effective fashion, the strategy will need to accomplish two tasks, each familiar to the international community: first, assess the host nation and, second, establish a goal toward which to build. To put it more in the vernacular, a cure without a diagnosis will be improbable; directions without destination will be random. In short, an effective approach will require an information business plan for the host nation. Figure 2 is a notional model for a stability and reconstruction information and communications business plan.

Figure 2: A notional model for a stability and reconstruction information and communications business plan.

The assessment phase of an information and communications business plan should begin before the intervention. It must include analyses of both information requirements and available information technology. Unlike humanitarian interventions, such as the relief effort for the December 26, 2004, tsunami, stability and reconstruction operations generally have long build-up periods, so there is time to prepare. An assessment would consider the pre-intervention state of information technology and information usage in the host nation. It is important to recognize that baselines will differ in different host nations. What can be accomplished in a country with an austere, pre-crisis baseline is likely considerably different from what can be accomplished in a more built-up, moderately established country. As an example, Bosnia is different from Afghanistan in terms of establishing an information business plan. Different baselines will generate different goals, and there will be no "one-size-fits-all" approach.

Some key elements of an information assessment will include evaluation of the host nation's telecommunications laws and regulations and communication infrastructures—land line telephone system, cell phone capacity, Internet availability. It should also address usage patterns, language and literacy issues, technical training of locals, and financial resources.

Once an assessment has been undertaken, goals will need to be set for operationalizing the information business plan. Generally, it will be useful to time-phase the goals into an initial deployment phase, a middle phase (getting-things-going phase), and a long-term (exit-by-intervenors) phase. A critical point throughout is that the intervenors' information business plan goals need to be in support of the overall goals for the host nation, and the host nation as promptly as possible will need to help generate those goals.

The initial deployment phase will require the intervenors to consider what deployable capabilities will be useful to help establish a host-nation element or elements. There are both structural information capabilities, such as deployable cell phone capacities and the use of satellites, and functional capabilities, such as "health care in a box," that need to be considered.

The virtue of preplanning is that key intervenors can rationalize their capacities in the early, usually chaotic days of an intervention by considering which capabilities each might

focus on. Equally important is to undertake such a discussion remembering that, first, numerous entities will already be in country with some capacities that can be utilized and that, second, host countries will likely have some capacity, and perhaps some significant capacity. Over the entirety of the intervention, the implementation of the information business plan likely will mean that the lead on different aspects of the plan will change. Broadly, one might expect a move from outside military intervenors to outside civilian intervenors to host nation, although the reality is likely to be more coordinated and complex. The transitions will occur over time, so there will be overlaps that need careful management. If it is understood from the beginning that there will be transitions in the way the plan is implemented, it will make for a more realistic and effective approach.

The middle phase of an information business plan for the host country will focus on five key elements. First is to *align the host country so that it is connected to the collaborative mechanisms used by the intervenors in some fashion*. While the key intervenors likely can use high-tech means, it may be that the host country will not be able to do so. An important task of an information business plan will be to allow for low-tech to high-tech connectivity. As an example, in Afghanistan, the literacy rate is so low that Internet use is necessarily limited and cell phone connectivity may be much more important. In fact, in Afghanistan, the cell phone is the lifeline communications capability. These points can be more broadly generalized: if the information business plan is to succeed, it must take account of the host nation's information culture and the related information technology culture.

A second element is to *help establish working government agencies*. Depending on the overall strategy, these could be central ministries or local/provincial offices. Information communications technology can be used to improve ministry effectiveness, especially to allow for an analytic approach through budgeting and transparency of expenditures. Those are crucial functions for the establishment of legitimate governance, and information technology can help each.

A third element for many stability operations will be to *increase connectivity and information flow between the central government and provincial/local governments*. Information communications technology can enhance this connectivity and information flow through, for example, the two-way flow of data and finances. It can also serve to extend government services and establish legitimacy of the government at all levels. Often, the cause of the crisis will have been differences between the central government and a region of the country, and working to bring warring elements together will be important. An information business plan can be an effective part of an overall effort.

A fourth element will often be to *provide certain important greater functionalities in government services to the populace*. While an information business plan may not be able to improve all functionalities significantly, health and education are two arenas of consequence in which such a plan can make an important difference. In the health arena, information technology can be used to build up local centers of health care, such as hospitals; support training of health care workers; and provide valuable functionalities, such as health surveillance systems. In the education arena, information technology can support curriculum establishment and the provision of instruction, as well as the training of teachers.

The fifth element is to *provide for the private-sector development of information capabilities*. Two of the most important issues are informed regulatory mechanisms and useful seed financing. An overly constrained regulatory environment will make it difficult for

private enterprise to operate at a profit. A properly structured set of incentives can help create an environment in which profit-making companies can contribute importantly to economic reconstruction. Seed money may be very important, especially in the early days of a stability operation, particularly to get local involvement in the development of the information business plan.

The middle phase of the plan often may be the equivalent of the medical "golden hour" for establishing a framework for effective use of I/ICT for the host nation. While the information flow may be limited, meeting expectations of the host government and population during this middle phase will be very important to longer-term success for the intervention and the host nation.

The middle phase will naturally flow over into the long-term phase for the host nation and the exit strategy for the intervenors. That part of the information business plan strategy should have at least three key elements. First, as noted above, the private sector should become a key element. Early establishment of a good public-private sector partnership is essential for success. In this regard, creating an environment in which there are commercial opportunities for information communications technology solutions, private sector telecom and IT firms will help seed economic revitalization. Second, the host nation will need to consider what role it will play in the development of a national information technology infrastructure. Models range from full privatization to early phase ownership to ongoing involvement. If state owned telecom and IT institutions are employed at the outset, it is important to have a clear agreement to privatize and plan for doing this in a timely manner—the earlier the better. Third, as part of their effort in country, intervenors will have established IT capabilities. Such facilities and datasets should not be automatically dismantled as the intervenors leave. Rather, they should be built as leave-behinds for local partners, both governmental and nongovernmental, whether commercial or non-profit. As part of the leave behind is the need for capacity building plans to ensure that the needed host-country ICT and management skills are available to sustain operations.

An I/ICT strategy includes people, content, and technology. In a stability and reconstruction operations, the information needs—the content of what must be provided in addition to the connectivity—of the host nation require consideration. Broadly speaking, those information content needs will fall into the categories of security, humanitarian, economic, governance/rule of law, and social.

In analyzing how such information needs should be fulfilled, an I/ICT strategy will recognize that the information element will support functional strategies for each of these arenas—all of which will have significant subparts. For example, the establishment of prosecutorial, court, and prison functions will have security and rule of law/governance aspects. Significant programs will be under way to help create each of these elements as part of a stability operation. Responding to the information needs of those programs has to be an affiliated strategic effort—or, to use the terms of the international community, needs to be aligned with the overall aims of the functional programs.

The specific needs may be provided with the use of information from one or more of the intervenors. In a variety of ways, information technology can be utilized to provide expert assistance. A simple example is maintaining an online list of experts. More sophisticated efforts can be established, such as a call-in center for the provision of various kinds of information. Research arrangements can be set up online, as can connectivity with key

national and international organizations, both governmental and nongovernmental, that are willing and able to provide assistance.

As is true for the technology itself, information needs change over time. In fact, the ability to provide information may become more important as the host nation develops its own capacities. The capacity to access such information may be developed in two parallel fashions. First, in a traditional approach there could be an office to help facilitate access to expert management. More recently, a distributed approach, such as Wikis and blogs, may be able to make a great deal of expert information available without a specific data manager, if the right information tools are provided.[14] Issues of trust and reliability will arise, but the community approach to providing information via the Internet has been very powerful in other arenas, and its use in stability and reconstruction operations should be encouraged.

The discussion of the management of information needs raises the important question of how to manage the I/ICT strategy in the course of the stability operation. Adoption of a strategic approach and even operational activities will be greatly facilitated by the establishment of a forward field organization. Ideally, this would be a joint Department of State-DOD function with the job of carrying out the information strategy in country. In stability and reconstruction operations, the organization likely would be collocated with the military command activity.

The role of the organization would include carrying out the U.S. Government aspects of the I/ICT strategy. In addition, the organization would collaborate with the organizations with which preplanning took place, including key countries, the UN, and major nongovernmental organizations. As promptly as possible, the organization will want to begin to work with the host nation, though precisely what that means will depend on the circumstances of the operation. As a forward community of interest is being set up, the organization will want to create mechanisms that add to the effort entities that have not been part of the preplanning. As discussed above, a hub type approach may be very valuable, as may more structured relationships. In addition, the organization will want to work with the public affairs office to facilitate interaction with the media and, most importantly, information for the public at large.

CONCLUSION

I/ICT can be important components for success in stability and reconstruction operations. To achieve successful results requires that a purposeful strategy be adopted to use these capabilities to the desired end of building up the host nation and to develop operational activities that effectively implement the strategy. A strategic approach causes coalition participants to undertake five key activities:

- Conduct pre-event activities with partners.
- Implement improved collaboration.
- Ensure improved data usability.
- Develop an information toolbox.
- Create a forward field information office.

Also, creating an overall focus to generate an effective host-nation information business plan consists of four actionable items:

- Assess host-nation information capacity.
- Build a host-nation information goal.
- Create immediate, medium, and long-term information capacities.
- Analyze information needs and develop methods to fulfill those needs.

Finally, opportunities to change the International and USG intervener community behavior and approaches to ICT reconstruction and development remain. Some key areas where changes need to be made are as follows:

- Policy actions.
    - Designate ICT an "essential service."
        - Recognize ICT as an engine of economic development
        - Agree on importance of telecoms and IT as an enabler of cross sector reconstruction and development
        - Elevate ICT investment priorities to be equivalent to roads, power, and water.
    - Ensure "political will" to coordinate and share civil-military ICT-related stability, reconstruction and development information.
- Strategies and plans.
    - Improve understanding of affected-nation information and related ICT business cultures.
    - Develop agreed coherent community strategies and plans for supporting and enabling affected-nation ICT reconstruction and development strategy and plans.
    - Improve management of the risks of protecting civilian and military elements and implementing reconstruction initiatives in hostile environments.
- Collaboration and information sharing.
    - Agree on mechanisms and processes to facilitate coordination and information sharing, including a shared situation awareness of reconstruction and development activities, especially for ICT.
    - Institutionalize agreed process.
    - Develop a concept of operation including common terminology.
    - Agree to implement shared ICT capability packages that enable and facilitate collaboration and information sharing.

These activities and items can generate an environment in which the information revolution can help create success in stability and reconstruction operations.

NOTES

[1] Frank Kramer, Stuart Starr and Larry Wentz, *I-Power: Using the Information Revolution for Success in Stability Operations*, Defense Horizons 55, Center for Technology and National Security Policy National Defense University, January 2007.

[2] Net-centric warfare, as defined by the Department of Defense Functional Capabilities Board, refers to: warfighting that networks all elements of an appropriately trained joint force; integrates their collective awareness, knowledge, and experience in order to rapidly create new capabilities, make superior decisions, and achieve a high level of agility and effectiveness in dynamic and uncertain operational environments.

[3] Department of Defense (DOD) Directive 3000.05, *Military Support for Stability, Security, Transition, and Reconstruction (SSTR) Operations*, Section 4.2, provides: "Stability operations . . . immediate goal . . . is to provide the local populace with security, restore essential services, and meet humanitarian needs. The long-term goal is to help develop indigenous capacity for securing essential services, a viable market economy, rule of law, democratic institutions, and a robust civil society." In this paper, the term *stability operations* is used per the DOD Directive to mean the full-spectrum of stabilization and reconstruction activities.

[4] World Bank, Operations Policy and Country Services, *Fragile States—Good Practices in Country Assistance Strategies*, December 19, 2005, vii, available at <www-wds.worldbank.org/external/ default/WDSContentServer/IW3P/ IB/2005/12/22/000090341_20051222094709/Rendered/PDF/34790.pdf>

[5] Organisation for Economic Co-operation and Development, Development Co-operation Directorate, Senior Level Forum on Development Effectiveness in Fragile States, Harmonisation and Alignment in Fragile States, December 17, 2004, 14, available at <www.oecd.org/dataoecd/20/56/34084353.pdf>.

[6] Ibid.

[7] In the discussion that follows, the focus will be on the implementation of an I/ICT strategy through the use of I/ICT for effectiveness, harmonization, and alignment—that is, to make the coalition and the host nation work more effectively. This focus is different from a strategic communications strategy, which is also a key element of an overall information strategy. While the importance of effective strategic communications has been well noted (by the Defense Science Board, among many others), how actually to make such communications effective in the context of stability operations is less than clear, and the authors of this paper are undertaking an additional ongoing study on that issue. The author, however, has come to a conclusion as to how to utilize I/ICT for harmonization, alignment, and effectiveness purposes, even apart from strategic communications. Those issues are the burden of this paper.

[8] For example the Office of Military Affairs was established to help bridge the gap between DOD and USAID and to help educate USAID personnel on military culture and to facilitate coordination. The Office of Infrastructure and Engineering is linked closely with the Army Corps of Engineers and is designed to emphasize infrastructure development. And the Bureau of Democracy, Conflict and Humanitarian Assistance has been reorganized to strengthen its capacity to act as U.S. Government lead in dealing with fragile states.

[9] The Leland Initiative, begun in June 1996, promotes the transfer and application of information technologies in Africa. The Digital Freedom Initiative was initiated in March 2003 with the aim of promoting economic growth in the developing world through the transfer of information technologies. The Last Mile Initiative was launched in April 2004. It seeks to expand access of the rural poor to communications technology and thus increase productivity and aid development.

[10] Jill L. Boardman and Donald W. Shuey, "Combined Enterprise Regional Information Exchange System (CENTRIXS); Supporting Coalition Warfare World-Wide," available at <www.au.af.mil/au/awc /awcgate/ccrp/centrixs.pdf>.

[11] Robert K. Ackerman, "Unclassified information New Key to Network Centricity," *SIGNAL Magazine* (September 2006), available at <www.afcea.org/signal/articles/templates/SIGNAL_Article_Template. asp? articleid=1185&zoneid=52>.

[12] DOD 3000.05, Sections 5.1.9, 5.7.1.

[13] Larry Wentz, *An ICT Primer: Information and Communication Technologies for Civil-Military Coordination in Disaster Relief and Stabilization and Reconstruction*, Defense and Technology Paper 31 (Washington, DC: Center for Technology and National Security Policy, July 2006), available at <www.ndu.edu/ctnsp/Def_Tech/DTP31%20ICT

%20Primer.pdf>.

[14] Wiki is a piece of server software that allows users to create and edit Web page content freely using any Web browser. Wiki supports hyperlinks and has a simple text syntax for creating new pages and crosslinks between internal pages on the fly.