INSS
INSTITUTE FOR NATIONAL STRATEGIC STUDIES

July 2013

DEFENSE HORIZONS
National Defense University

Sharing to Succeed: Lessons from Open Information-sharing Projects in Afghanistan

by Linton Wells II, James Bosworth, John Crowley, and Rebecca Linder Blachly

About the Authors

Linton Wells II is the Director of the Center for Technology and National Security Policy, Institute for National Strategic Studies, at the National Defense University (NDU). James Bosworth is a Freelance Writer and Consultant based in Managua, Nicaragua. John Crowley is an Information-sharing Analyst at NDU and Research Fellow in the Harvard Humanitarian Initiative. Rebecca Linder Blachly is Director of Advancement, International Programs, and Studies at the University of Illinois at Urbana-Champaign.

Key Points

- **Unless U.S. and coalition forces can share information with the populations they seek to influence in complex civil-military operations, they cannot achieve the goals for which they were committed.**
- **Information, communications, and related support structures influence all aspects of complex operations and need to be treated as critical infrastructures and essential services but rarely are.**
- **Open information-sharing projects require sustained leadership interest plus shared and stable priorities among many parties. Absent this emphasis, changes in personnel, mission priorities, and funding levels will make it hard to develop, transition, and sustain any such effort.**
- **Observations from information-sharing projects in Afghanistan suggest several ways to change behaviors that can turn lessons observed thus far into lessons actually learned.**

The sharing of information in complex civil-military operations[1] is important, yet actors rarely do it well. U.S. and allied military forces must be able to communicate, collaborate, and exchange information effectively with the local populations they seek to influence, or they cannot achieve the goals for which they have been committed. Nonetheless, experience from stability operations in Afghanistan and Iraq, numerous humanitarian assistance/disaster relief missions, and efforts to build the capacity of foreign partners suggest that effective information-sharing is much harder than might be expected. This paper sheds light on the difficulties of setting up and sustaining projects to share information in such situations and suggests ways to do better in the future.

The reasons are straightforward. Government practitioners are unfamiliar with many of the technical solutions to ineffective information-sharing. Moreover, information-sharing runs counter to long-held information-controlling habits. Incentives rarely reward sharing and instead punish leaks. Projects that try to mitigate information-sharing problems typically take a long time to develop, need broad coalitions to implement, and have results that are hard to measure and attribute. Many of the stakeholders do not have institutional ties and some actively seek to minimize relationships with each other. As has often been seen in projects in Afghanistan, changes in personnel and government priorities can make projects hard to sustain. Collectively, the impacts have been detrimental to information-sharing.

This paper draws on examples from Afghanistan to highlight some lessons that members of diverse organizations have observed over a number of years.[2]

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUL 2013		**00-00-2013 to 00-00-2013**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Sharing to Succeed: Lessons from Open Information-sharing Projects in Afghanistan	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University,Institute for National Strategic Studies (INSS),300 Fifth Avenue, Fort Lesley J. McNair,Washington,DC,20319**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**12**	

The first case study focuses on an informal information-sharing project near Jalalabad in Nangarhar Province that builds on personal relationships and technical infrastructures developed since 2006. It is colloquially referred to as the Nangarhar pilot and continues to unfold. The second project, termed UnityNet, went through various phases. A combination of organizations in Washington and Kabul began UnityNet in mid-2010 to build on experiences from Nangarhar and elsewhere to develop a globally deployable, sustainable program to share population-centric, or "white," information. However, personnel turned over and disagreements developed over the purpose and scope of the project. Efforts to move UnityNet away from its original white information focus and repurpose it for "green" (government-military) intelligence collection raised concerns that associating with it could jeopardize people in the field who had intended to support only population-centric information-sharing. In early 2011, components of the International Security Assistance Force (ISAF) in Afghanistan proposed an implementation effort under UnityNet, called UnityNet Afghanistan, to support Village Stability Operations (VSO). However, the continued emphasis on green intelligence reraised the same concerns about the safety of associated partners and UnityNet was terminated. The third case relates to a new follow-on project, focused on both green and white information, that was named Jade-A in June 2011. An assessment team evaluated its status in early 2012.

The origins of the various efforts along with examples of their activities and descriptions of how different kinds of open information were accessed and shared are outlined below. Some of the organizational challenges that each approach encountered and the lessons available to be learned if behaviors can be changed—at several levels—are also included. This is important since the lessons are similar to those derived from other contingencies and may be applicable in other regions in the future.

It is also vital to distinguish some of the categories of information this paper addresses. Classified information involves a variety of dissemination restrictions. Confidential, secret, and top secret are the most well known, and each has its own handling rules.[3] Less sensitive official information may be designated *un*classified.[4] However, nongovernmental organizations (NGOs), international organizations, local villagers, and commercial firms continually exchange other important kinds of information completely outside the reach of government classification authorities. This information is termed *non*classified.[5] Such information flows can provide insights into aspects of population-centric campaigns that may not be routinely accessible to governments. Not only is it important for governments to support this kind of sharing, but they should also participate by providing information, such as imagery and maps, as well as education about how to use it to improve situational awareness for all. Collectively, this paper refers to unclassified and nonclassified information as open information and concludes with recommendations on how to share open information more effectively.

Benefits of and Impediments to Information-sharing

In early 2010, the Deputy Chief of Staff of Intelligence for ISAF, then–Major General Michael T. Flynn, USA, along with coauthors Matt Pottinger and Paul D. Bachelor published *Fixing Intel: A Blueprint for Making Intel Relevant in Afghanistan*. The authors argued that the coalition in Afghanistan had been too focused on intelligence about enemy forces and actions, or "red" information. The paper noted, "a single-minded obsession with IEDs [improvised explosive devices] that while understandable is inexcusable if it causes commanders to fail to outsmart the insurgency and wrest away the initiative."[6] Instead, particularly in a population-centric campaign, the authors recommended that the coalition focus more on collecting information about local populations—white activities—and host government structures, policies, and personnel—green activities.[7] Much of this white and green information would begin as nonclassified, incorporating knowledge that might be critical for success in population-centric operations. Nonetheless, in

the context of *Fixing Intel*, the collection of white information, even though population-centric, is still an intelligence function. This needs to be kept in mind when dealing with NGOs and others who might be wary of dealing with the military.

Independent activities by NGOs, international organizations, and others can generate extensive nonclassified information that can provide links to local conditions that may be beyond the normal reach of military operators or intelligence-gathering players. At the same time, government entities often have information including maps, imagery, and historic data that can be useful to NGOs, local populations, and commercial firms. Sharing these can benefit many parties and help overcome mutual suspicions and misunderstandings, as well as legitimate differences of opinion and objectives.

Open information is not restricted by explicit classification, but its sharing is frequently limited in several ways. NGOs and sometimes even coalition partners complain that open information provided to government sources quickly gets posted to classified networks for intragovernment sharing but rarely reemerges from them in unclassified form even though the information could contribute to common objectives. In other cases, authorities may classify aggregated amounts of open information "by compilation," though the rules for that are rarely clear.[8] The net result is that many outsiders are reluctant to share information with the government because they see the knowledge flow as a "one-way street."[9] That only compounds the natural concerns of NGOs and other private organizations working in hazardous environments. They believe they are risking vital relationships, and maybe their existence, to associate with the military while getting little in return.[10] Even in the best of times they work hard to maintain a neutral stance, believing strongly that neutrality is key not only to their operational effectiveness but also to the safety of their people. However, if the collective result is a lack of shared situational awareness, it could increase the risks to all.

Other restrictions to sharing information may arise as well. Budgetary rules can impede exchanges as arcane budget classifications sometimes keep money from being spent on such things as key enabling information communications technologies (ICT)[11] or fuel for generators. Future deliberate leaks of classified information, such as occurred through WikiLeaks, will probably lead to further calls to reduce sharing. As this paper notes later, though the Nangarhar pilot project had no connection to classified information systems, government people still expressed concerns about possible compromises and misuses, which complicated open information-sharing.

In trying to bridge the cultural gap between coalition forces and NGOs and other nongovernment entities, it is useful to understand that "intelligence" may be considered as "information" in a specific context. Consider a request from a local party for an ambulance to take a wounded citizen to a hospital. The original request would clearly be nonclassified information. The same information could become intelligence if it was acquired by a military unit and helped expose the state of a conflict. At the same time, NGOs and other civilian organizations use official information for their own purposes. The fact that government entities similarly make use of nonclassified information should not be a cause for these organizations to censure such government actions.

NGOs and sometimes even coalition partners complain that open information provided to government sources quickly gets posted to classified networks

It is not surprising that NGOs and similar organizations are wary of the "militarization" of their information as intelligence even though they may grudgingly admit that broadly based situational awareness is part of providing security. Governments, in turn, resent the unwillingness of NGOs to share their information, often not recognizing the genuine concerns the organizations have

about putting their own people and those they seek to help at risk. In any case, given that the same facts could have different uses depending on context, all parties should understand the mutual benefits of shared situational awareness.

Successes and Shortfalls

In November 2005, a key Department of Defense (DOD) directive formalized the importance of support to stability, security, transition, and reconstruction operations, now commonly called stability operations, and gave them comparable priority, conceptually at least, with major combat operations.[12] This included direction to the U.S. military "to collaborate with other U.S. Government . . . agencies and with foreign governments and security forces, international governmental organizations, [NGOs], and private sector firms as appropriate to plan, prepare for, and conduct stability operations."[13] The directive also tasked the military to "develop policies and systems for sharing classified and unclassified information during stability operations among [these same components]."[14] At about the same time, the Office of the Assistant Secretary of Defense for Networks and Information Integration and DOD's chief information officer increased support for efforts to improve information-sharing connections among the disparate actors involved in postdisaster and postconflict environments.[15] The Nangarhar pilot project was an example of how this kind of sharing might work in the field.

The Nangarhar Pilot Project. In 2006, several individuals with ties to various NGOs and DOD went to Nangarhar Province to find open information-sharing solutions that could be useful in Afghan operational environments.[16] This group, called the Synergy Strike Force (SSF),[17] has continued these visits several times a year ever since. The SSF consisted of an eclectic array of individuals with a wide range of talents who were interested in helping Afghanistan build toward peace and stability. The SSF hoped to identify opportunities for collaboration, identify potential partners, and facilitate accomplishment of shared goals. To help implement the pilot project, SSF members chose a guesthouse near Jalalabad as a "neutral space" where social, cultural, and bureaucratic barriers could be reduced and a technological infrastructure for information-sharing could bring significant value. Initially, the team provided connectivity to the guesthouse through Internet hookups and technological infrastructure. Throughout the next several years, the team added participants and enhanced the level of information-sharing. The pilot identified three basic findings about effective information-sharing.

The first finding was that *people are more important than technology*. The selection of people on all sides is therefore key. In practice, this required having stakeholders who could bridge social and cultural divides between coalition forces and Afghans. In that context, a review of lessons from the pilot identified two key positions: a synergist outside of government and a facilitator inside. The relationship between those members is essential.

The *synergist* bridges gaps among systems, organizations, and individuals and engages in problem-solving with local stakeholders. Synergists are almost always chosen from outside the governmental-bureaucratic system, are technologically knowledgeable, and must be able to work with a wide range of partners to cross social, cultural, language, and technological divides in austere environments. That is not to say that a synergist has total freedom of action, an unfettered call on resources, and no accountability but rather that it is vital to engage someone who can work "outside the wire" with nontraditional mission participants. The *facilitator* works within the governmental-bureaucratic system and is able and inclined to support the synergy operation to the extent possible. Through knowledge of key bureaucracies and procedures, the facilitator can help the operation overcome impediments. Thus, the two must work together. Synergists can engage in creative local problem-solving only because facilitators have provided the operational space and perhaps some resources.

In addition to the synergist-facilitator dyad, a central necessity for open information-sharing has been developing personal relationships early with actors who are

seen as working in the local community's best interest rather than for their own political agendas. An important lesson from the commendable La Jolla Golden Triangle Rotary Club initiative and the San Diego–Jalalabad Sister City Program[18] has been the need to find the right institutions to serve as partners and provide the organizational credibility on which the extraordinary work of the committed individuals involved can build. Being able to extend the relationships of organizations that already have local contacts greatly increases the likelihood of successful information-sharing and synergy.

The second finding is that *open Internet connectivity itself can facilitate social collaboration and knowledge creation*. Many DOD and NGO personnel did not have access to the open Internet in their work environments because they could not afford wideband connectivity in the field. Providing bandwidth, strengthening local computing power, working with available technologies even if they are only cell phones, and providing stable power supplies help reinforce personal relationships that facilitate further sharing. Increased access to connectivity also acts as a catalyst for greater cooperation and innovation.

The third finding is that *incentives are important*. The combination of maps, imagery, an open-hosting platform (computer), and bandwidth, as well as food, drink, and a neutral social space, brought together a diverse set of actors at the Nangarhar pilot site who then shared information across their organizational boundaries. Incentives varied with attendees—alcohol was not served when Afghans were present, for example. The group practiced a form of radical inclusion, allowing nearly anyone with peaceful intentions to enter the neutral space and collaborate with others.[19] The synergists used this space to focus on identifying and bringing in groups and individuals who wanted to collaborate. They did not waste significant energy trying to change the minds of those reluctant to share. The motto was "Save the willing first."

Opinions differ as to the extent that this sharing has supported U.S. Government and coalition objectives, but participants believe the Nangarhar pilot has not only provided valuable exchanges[20] but also demonstrated that more parties find constructive uses for information and network access than destructive uses. Access provides opportunities to populate networks with beneficial data and to address information that could pose a risk. Providers or managers can filter truly sensitive imagery before it is disseminated, but activities at the guesthouse over several years indicate that erring on the side of sharing imagery has had generally positive effects without incurring the negative consequences detractors have postulated.[21]

UnityNet. In the fall of 2009, the Office of the Secretary of Defense's Intelligence, Surveillance, and Reconnaissance (ISR) Task Force (TF) in Washington, DC, designated funding for "Non-Traditional Sources"

the Nangarhar pilot has demonstrated that more parties find constructive uses for information and network access than destructive uses

and an "Open Sharing Environment" quick reaction capability concept. As noted earlier, the publication of the *Fixing Intel* paper in January 2010 had a significant impact on thinking about the uses of green and white information in the Afghan War. This led directly to a white paper on a concept called UnityNet.[22] According to the preface:

> *"Fixing Intel" . . . served as a tipping point in operationalizing concepts of Counterinsurgency (COIN) and Stability* [operations] *doctrine in a way that will forever change how we view our military role in Afghanistan and other areas of conflict throughout the world. A new tested and proven information-sharing model now exists that directly supports the concepts that "Fixing Intel" establishes by providing an ISR platform that "senses" population-centric atmospherics and information critical to COIN and stability*

operations. This model, termed Unity Net, enables host-nation, open-information-sharing environments in areas around the world of interest to the United States. Unity Net's primary function is to expose grassroots, population-centric, socio-economic and governance information that is not readily accessible to military commanders, civilian policymakers, and other civilian aid organizations seeking to execute development programs, stability operations or counterinsurgency doctrine.[23]

The white paper concluded that the "Jalalabad experience of bringing people and technology together in an open-source process model has evolved into a force that has brought significant change to Nangarhar Province.

UnityNet initially was seen as a way of applying the ideas, concepts, and experiences from the Nangarhar pilot to other Afghan regions and even other theaters

It is this experience that we propose to emulate in the future form of UnityNet." As described above, through the exposure of white information, UnityNet initially was seen as a way of applying the ideas, concepts, and experiences from the Nangarhar pilot to other Afghan regions and even other theaters.

A series of developments, mainly in Afghanistan, undercut support for UnityNet. Personnel rotations reduced interest in previously approved projects while changes in the security situation reduced the priority of white information. Additionally, since intelligence organizations and funding supported UnityNet, return-on-investment calculations had to be based entirely on the project's value to intelligence, not on a more broadly based view of its contributions to the entire population-centric campaign. The shift of the intelligence emphasis to red and green activities from a white focus reduced UnityNet's perceived value. Accordingly, the ISR TF terminated the use of the term *UnityNet* in December 2010, as well as the quick reaction capability associated with it.

Nonetheless, in late March 2011, ISAF submitted an operational needs statement for a project called UnityNet Afghanistan to U.S. Central Command as a way to implement a variant of the original UnityNet concept.[24] UnityNet Afghanistan was meant to serve as an information-sharing and collaboration medium among the various levels of the Afghan government, Afghanistan National Security Forces, ISAF coalition members, and other mission partners in support of governance, security, and stability operations. It was to use the Internet to facilitate both formal and informal exchanges of essential green and white information among local, district, provincial, regional, and national populations and organizations in underserved rural and urban areas of Afghanistan. Another goal was to help develop the capacity of Afghan governance to share information, with a particular emphasis on support to Afghan governance and security forces. To encourage long-term success, ISAF intended UnityNet Afghanistan to be sustainable at a set of designated sites with a minimum of 12 months of operational support provided once installation was complete.

By late spring 2011, a combination of factors led to UnityNet Afghanistan being downscoped. Essentially it became the implementation of Internet access at five sites, along the lines of the architecture and template from the Nangarhar pilot (described in more detail below). However, the lack of an agreed concept of operations bedeviled the project, and there were questions about what the scope of an analytical assessment should be. The questions included whether the assessment should cover the role of voice (cell phone), data (information technology [IT]), or the amount of effort that could be devoted to peripheral capabilities such as power and buildings, within the authorities of Overseas Contingency Operations funds. Moreover, participants in and out of government still had concerns that the shift to green intelligence collection could endanger those in

the field seen as being associated only with white population-centric information-sharing projects. Because of these problems, the UnityNet Afghanistan project was also suspended.

Jade-A. In the spring of 2011, distinct from the UnityNet Afghanistan efforts described above, Combined Forces Special Operations Component Command–Afghanistan (CFSOCC-A) outlined requirements for a project to support VSO by providing voice, video, data, and other related support elements such as power sources to facilitate collaboration, information-sharing, and governance while supporting mission partners and district-level governance in Afghanistan. This was a far more focused requirement than UnityNet or UnityNet Afghanistan, and it became known as Jade-A.[25]

VSO uses security, governance, and development lines of operations to harden at-risk villages and communities against insurgent influence, intimidation, and ideology. Jade-A was planned to support VSO by using ICT tools and Internet connectivity to facilitate both formal and informal exchanges including essential green and white information among local, district, provincial, regional, and national populations and organizations in underserved rural and urban areas of Afghanistan. The goal was to enable governance and socioeconomic development, which are essential components of stability operations and counterinsurgency.

The notional Jade-A architecture was derived primarily from a draft of a 2010 UnityNet Strategic Plan and refined in a November 2010 presentation to senior leaders in Kabul and Washington, DC. The initial Internet access concept matured into a wireless IT network supporting district-level governance and security needs as well as selected access for schools and medical clinics, providing an opportunity to collect both green and white information. Jade-A had four objectives:

- deploy a common medium for exchanging reports and essential information among local, district, provincial, and national elements
- increase the level of communication among participating organizations at designated locations enabling them to exchange information and identify and resolve information-sharing problems
- support development of sustainable formal and informal information-sharing environments among participating partners
- create a useful leave-behind capability for the government, security forces, and people of Afghanistan.

Coalition forces in coordination with CFSOCC-A selected five Jade-A pilot sites. They based site selection on VSO district-level security, stability assessments and objectives, and strategic location. They selected locations in four strategic provinces—one in the west, two in the south, and one in the east. Since Jade-A capabilities were intended to complement CFSOCC-A VSO, the introduction of Jade-A was coordinated carefully through district governments and security services by the CFSOCC-A representative. In addition to the district sites, a Jade-A test bed and hub was established at Camp Julien, Kabul. The hub provided service to U.S. Consolidated Stability Operations Center analysts and a school for underprivileged children sponsored by the Ministry of Borders and Tribal Affairs.

the initial Internet access concept matured into a wireless IT network supporting district-level governance and security needs

The Center for Technology and National Security Policy at the National Defense University commissioned a team to conduct site assessments on behalf of the task force, and it went to Afghanistan in January 2012. To help theater leadership determine whether the Jade-A pilot project added enough value to remain in service, coalition representatives asked that the report primarily assess the status of the Jade-A pilot rather than broad

VSO support requirements. After several adjustments in tasking, the team was asked to use the assessment process to address three specific questions: 1) Does Jade-A provide value to the Intelligence Community? 2) Is Jade-A of value to Afghans, and how is it being used? 3) Can Jade-A be transitioned to and sustained by Afghans?

The assessment team found that even with limited insights into operational experience from recent implementation, Jade-A clearly had the potential to provide value to the Intelligence Community. The challenge was to put in place a concept of operations, strategy, plan, organization, and the resources to engage appropriately and actively to develop a more informed understanding of how to use and leverage Jade-A's value. The Special Operations Task Force–West team at Shindand was especially supportive.

Afghans were enthusiastic about using Jade-A to improve information-sharing, office operations, and the way they do business

Second, Afghans showed a high level of interest in Jade-A capabilities. They were enthusiastic about using Jade-A to improve information-sharing, office operations, and the way they do business. However, they asked for training and mentoring to improve computer and Internet skills and wanted to use IT to enhance business processes, support information exchange among players, share information with elements in each provincial headquarters, and improve the efficiency and effectiveness of organization operations.

Finally, the team believed that Afghans could be trained to sustain Jade-A. At the time, however (early 2012), the district-level Afghan government teams were not ready to accept operational and business responsibilities, and they were probably not capable of sustaining Jade-A as an operational capability unless they could contract a local vendor to do it for them. This lack of capacity was in part an IT skills issue, but it also extended to a lack of IT business practices and business process skills to take over budgeting, business plans, and the operation and sustainment of the network services. Provision of reliable and sustainable power was another challenge in terms of a transition plan. In sum, there was a need for a strategy to ensure transition and sustainment.

Assessing the Impact of Information Flows

Assessment approaches need attention early in any project and refinement throughout its life. At a basic level, metrics for these types of operations can include information such as the amount of data shared, bandwidth available, attendance at social events, and positive or negative responses to the initiative by those working in the region. These can be measured by comments in communications or surveys. However, such metrics do not cover the most important aspects of synergy operations: social relationships and their development over time. Most metrics are quantitative measurements of the attribute of a noun, capturing its current state, velocity, or rate of change when acted upon by an outside force. Synergy operations, on the other hand, focus mainly on the existence and rate of creation of relationships among nouns, usually among people and organizations. Such precise metrics have not yet been developed or validated. In the interim, the assessment approaches that should be followed while more precise measures of effectiveness are developed must include a focus on human relationships and improving the ability to work with unstructured data.

Three principles of information-sharing suggest useful interim metrics. These principles were formulated by one of the participants in the Nangarhar pilot, Todd Huffman, who had extensive collaborative experience in many environments. If these principles are not followed, the effectiveness of data-sharing will be blunted over time. Similarly, the wariness between government and nongovernmental parties will continue if data-sharing between

them is not reciprocal. At the same time, effective data-sharing creates a positive feedback loop among the parties and can offer large and far-reaching benefits in terms of accuracy and credibility. The three principles are:

- create immediate value for anyone contributing data; contributors should get an immediate return for their efforts
- return contributors' data to them with improvements; any data that goes in should be available to be downloaded back out again; furthermore, any data should come back better than it went in
- share derivative works such as analyses, spreadsheets, charts, and reports with the data-sharing community; urge users who create derivative works from shared data to contribute their products back to the group.[26]

These principles suggest that the best measurements of performance and effectiveness for such operations are not easily quantified, but progress over time should be observable by the synergists and others working on the project. The most important goal is to measure the quality and durability of relationships built through the efforts of the team, to which social network analytics may contribute.

Additional and more quantifiable measures of effectiveness may focus on the quantity and quality of data-sharing and participation at the neutral site, recognizing the caveat noted above that the social networks and trust built through information-sharing may be more important and enduring than numbers indicate. Certain negative indicators including the inability to sustain technological solutions or bandwidth, or a hostile reception by local organizations, should be early red flags for projects and indications that major changes or withdrawal should be considered.

Template for Information-sharing

The ideas, concepts, and experiences from the Nangarhar pilot suggest an initial template for future operations in other locations as they become accessible. The template is designed to be adaptable and iterative. It could be adjusted to address local circumstances and could also incorporate lessons learned from future operations. The assessment team, SSF, and others should focus the template on an initial 90-day project setup in which the relationship-building efforts are to be conducted and the enabling technology installed. While creating relationships for information-sharing usually takes longer than 90 days, the model contains the principles noted above that attempt to capture initial indicators of success as well as red flags that indicate a project should be modified or cut. Its five major elements are:

- Personnel. Information-sharing operations require both an external synergist and one or more government facilitators, as described earlier. Typically, two levels of facilitators are needed: one to address issues at senior levels and the other working closer to the field to provide logistic and other support as needed.

the ideas, concepts, and experiences from the Nangarhar pilot suggest an initial template for future operations in other locations

- Neutral sites. A candidate site should be identified based on three elements: a need that can be met by information-sharing; mobility (freedom of movement by all parties); and a social fabric open to accepting such collaboration. Those working on the project should use their experience and knowledge to judge whether a proposed location will be suitable.

- Partners. Successful information-sharing operations generally encourage anyone to join who would be a productive participant. In the early stages, energy should be spent identifying those who want to be included rather than trying to persuade those who are reluctant to participate. While an ideal system would have the same

people interacting across time, synergy should be built on the expectation of high turnover in staff, enhancing the importance of institutional memory and relationship networks to a project's continued success—hence the need to capture that knowledge and save it for others to reference via a hosted open platform.

◆ Connectivity. Most complex operations proceed without a way to share information across organizations, or even among elements of the same organization. This limitation derives both from issues of connectivity and specific policies limiting information flow over existing pathways. The synergist needs to cross-ventilate these stovepipes, building relationships that function as trusted pathways for information flow and enabling those relationships to communicate over newly established information and communication technologies infrastructures.

◆ Iterative project cycles. Because information-sharing operations are built around the connection of people and the construction of trusted networks in a dynamic environment, they are not linear projects. Instead, they proceed through what may be thought of as iterative cycles. The synergist must reallocate effort and resources to dynamics that are working well. These dynamics can change dramatically in complex operations, especially as staffs rotate in and out of theater, new problems challenge existing assumptions, and new opportunities arise. Operations in these environments become cycles, measurable by the success with which the synergist and partners adapt and make progress in support of productive collaborations and mutually valued objectives.

Conclusion

This study leads to several broad conclusions and specific observations. To begin, the U.S. and allied national security community, especially policymakers, commanders, and ambassadors, must treat information-sharing as a critical enabler to mission success in population-centric environments. Absent this emphasis, changes in personnel, mission priorities, and funding levels would make it hard to develop, transition, and sustain any information-sharing program.

Information-sharing project leaders should engage key operational leaders and staff before they deploy and make them participants in the project. This also could help outgoing leaders who have had non-traditional information-sharing projects to get buy-in from successors. Often new commanders will start their own projects while downplaying or ignoring their predecessor's initiatives. Staff turnover certainly affected UnityNet.

Projects need to have broad bases of support from multiple directorates and agencies. Project leaders should seek facilitators in several key directorates of the participating organizations. It also is important to have the support of the appropriate ministries of the host nation.

DOD and coalition members need high-level support and policy guidance to engage in "responsible" information-sharing. Success requires that national security institutions themselves develop some level of tolerance for the risks of these kinds of sharing activities.

Cooperative arrangements could make coalition members and NGOs work more effectively toward creating stable and secure conditions. When international actors share situational awareness and lessons learned, expertise is less likely to be lost in the rapid turnovers characteristic of turbulent settings. When information is more available, it empowers decisionmaking at all levels, reduces redundancies, and helps create new opportunities for collaboration.

The Nangarhar pilot established relationships, provided connectivity for actors on the ground, incentivized information-sharing, and acted as a catalyst for increased coordination, connectivity, and collaboration. The essential features to support these tasks include synergists, facilitators, partners, neutral spaces, social networks, and technical connectivity. With all these in place, the project could be refined iteratively and adjusted to meet changing circumstances and local needs. It would be useful for policy guidance to be issued at appropriate levels among

key participants to encourage elements that contribute to success. This could facilitate more frequent synergy operations by the international community. However, since there will never be "unity of command" in complex civil-military operations, "unity of effort" must be encouraged at every opportunity. Policies that encourage collaboration could go a long way to this end.

At the same time, solutions that promote cooperation need to recognize that there always will be changing priorities among red, green, and white information, differing local security situations, and personnel turnovers that may affect the level of official support for synergy operations over time. Practitioners need to design programs to be inoculated against these predictable challenges. They also need to address the inevitable gaps in trust created by the "information vs. intelligence" issue continuously. Open information-sharing is not the same as white intelligence collection. All parties need to promote a better understanding of different organizations' information needs and the impact those needs may have on others.

The lessons observed and best practices outlined here apply to a wide range of contexts and geographic areas. Accordingly, they should inform policymakers and operators both in and out of government. That said, practitioners must use combinations of training, exercises, and education to turn the lessons observed into lessons genuinely learned.

The basic principle is valid anywhere: incentivized, responsible sharing of open information is a core element in building sustainable socioeconomic capacity in partner nations, whether in contested or uncontested environments.

Acknowledgments

The authors would like to thank Dr. Dave Warner, Mr. Michael C. Davies, and Mr. Andrew Masciola for their help in developing this paper.

Notes

[1] *Complex operations* are defined as those that require close civil-military planning and cooperation including stability operations, humanitarian assistance and disaster relief at home and abroad, and building the capacity of partner nations when civil-military activities are involved. This definition is adapted from Hans Binnendijk and Patrick M. Cronin, eds., *Civilian Surge: Key to Complex Operations* (Washington, DC: NDU Press, 2009), 10. This differs from most official definitions, which focus on subsets of this space. But since many similar capabilities and procedures can be applied to multiple missions, there is value in addressing them comprehensively.

[2] Observers include representatives from the Office of the Secretary of Defense, National Defense University, Defense Information Systems Agency, nongovernmental organizations (NGOs), and others.

[3] For definitions of each level, see Department of Defense (DOD) Manual Number 5200.01, vol. 1, *DoD Information Security Program: Overview, Classification, and Declassification* (Washington, DC: DOD, February 24, 2012), 34.

[4] Even if unclassified, there still may be sharing restrictions, such as the "for official use only" caveat or other forms of "controlled unclassified information." See DOD 5200.01, vol. 1, 69, and vol. 4.

[5] *Nonclassified* is not defined in DOD security regulations. The term is used to highlight the need for U.S. Government cultures, particularly those of DOD and the Intelligence Community, to take into account the kind of information that may be important to the campaign but does not normally get much attention.

[6] Michael T. Flynn, Matt Pottinger, and Paul D. Batchelor, *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan* (Washington, DC: Center for a New American Security, 2010), 24.

[7] Usually, "Fusion Centers and CJ2 shops are overwhelmingly focused on 'red' activity—concerning the enemy—devoting relatively little effort to 'white' activity—the Afghan population, economy, development, and government." Ibid., 21.

[8] See DOD 5200.01, vol. 4, 12, 18, 37. Whether such "classification by compilation" can be done systematically or controlled in an Internet age remains to be seen.

[9] In about 2005, DOD initiated a network project called "harmonieweb.org" to encourage information-sharing with nontraditional mission participants (such as NGOs). During a meeting with DOD officials in 2011, an NGO representative began the conversation with "Don't ever ask us to use harmonieweb!" The reason was, "We never get anything back. Everything we provide to the government disappears into a black hole."

[10] For a more in-depth discussion of these issues, see Solomon Major, "Cross Roads or Cross Purposes? Tensions Between Military and Humanitarian Providers," *Parameters* 42, no. 2 (Summer 2012), 86–96; Also see "Guidelines for Relations Between U.S. Armed Forces and Non-Governmental Humanitarian Organizations in Hostile or Potentially Hostile Environments," *Interaction.org*, January 2011, available at <www.interaction.org/sites/default/files/Sec16_2011_FABB_Policy%20Paper_CivMil-Guidelines.pdf>.

[11] For example, funds for bandwidth come from different accounts than those for hardware and software.

[12] DOD Directive 3000.05, *Military Support for Stability, Security, Transition and Reconstruction (SSTR) Operations*, November 28, 2005, available at <www.fas.org/irp/doddir/dod/d3000_05.pdf>. This directive was reissued as Instruction 3000.05, *Stability Operations*, September 16, 2009, available at <www.dtic.mil/whs/directives/corres/pdf/300005p.pdf>.

[13] International organizations, NGOs, and private-sector firms do not conduct stability operations, but the military may interact with them in the course of such activities.

[14] DOD Instruction 3000.05, 9.

[15] A history of these efforts is outlined in Linton Wells II et al., *STAR-TIDES and Starfish Networks: Supporting Stressed Populations with Distributed Talent*, Defense Horizons 70 (Washington, DC: NDU Press, December 2009), 6–7, available at <www.ndu.edu/CTNSP/docUploaded/DH%2070.pdf>.

[16] These efforts are described in Chickasaw Nation Industries Technical Services (CNITS), LLC, *Research and Analysis Project for UNCLASSIFIED Information-sharing in Afghanistan: A Model for U.S. Military and Coalition Commanders, the U.S. Intelligence Community, and U.S. Homeland Security* (Albuquerque, NM: CNITS, January 28, 2011).

[17] *Synergy* is defined as two or more people collaborating to achieve a result that could not be achieved individually. *Synergy operation* is used to refer to an operation directed at improving the connectivity, coordination, and collaboration of complex operations in contested environments.

[18] San Diego and Jalalabad have been sister cities since 2004. See <www.sandiegojalalabadsistercities.org/>; Claire Harlin, "Del Mar Man Meets Afghanistan President Karzai," *Del Mar Times*, May 29, 2012, available at <www.delmartimes.net/2012/05/29/del-mar-man-meets-afghanistan-president-karzai/>.

[19] A *neutral space* is a physical location that no actor overtly tries to control, though informal control mechanisms usually are in place. Not all encounters will take place here, but it functions as the hub for a social network and a virtual space that goes beyond the physical infrastructure.

[20] Intelligence Community leaders were initially supportive of the pilot project and its data-sharing innovations, but some intelligence personnel in Afghanistan subsequently came to believe that much of the shared information was either redundant or less applicable to intelligence needs as their focus shifted from white activities back toward green and red data. It is unclear that a systematic, as opposed to an anecdotal, analysis of the Nangarhar pilot data has ever been done by the U.S. Government.

[21] As an example of how an open information-sharing environment helped to avert a potentially destructive situation, a road was being built near the Tora Bora mountains. The construction would have entailed rolling equipment over a cemetery. Members of the United Nations Office for Project Services had already built a relationship with villagers and were able to show them high-resolution imagery obtained through interactions at the Jalalabad project house. The images were viewed at a shura so elders could be shown that in order to build the road, the only place for trucks to turn around was in the cemetery. The elders asked for time to relocate their dead before construction. A peaceful resolution was enabled by freely available imagery that allowed a local governance structure to make the decision.

[22] Gary H. Thompson and David W. Muench, *UnityNet-—A Globally Deployable Sensor for White Information* (Washington, DC: Defense Intelligence Agency, May 5, 2010). Also see the commentary by Linton Wells II, "UnityNet Offers Information-sharing Boon," *SIGNAL Magazine* 64, no. 12 (August 2010), 88. Sometimes the concept was written as Unity Net.

[23] Thompson and Muench, 1. Civil affairs and special operations forces also collect population-centric and other information for commanders.

[24] The full operational needs statement for UnityNet Afghanistan is North Atlantic Treaty Organization Restricted. The account above is based on an unclassified summary. The statement references International Security Assistance Force Headquarters Fragmentary Order 046, *Establishment of the Civilian-Military Integration Program in Afghanistan*, February 26, 2011.

[25] Since the project was to focus on a mix of white and green information, the variable mix of green and white was termed *Jade*, with the *A* representing Afghanistan.

[26] Tyler M. Koziol et al, "Information-sharing in Village Stability Operations: Field Experiences and Policy Considerations," *Risk, Hazards & Crisis in Public Policy* 2, no. 2 (2011), 8.

INSTITUTE FOR NATIONAL STRATEGIC STUDIES

The Center for Technology and National Security Policy (CTNSP) within the Institute for National Strategic Studies helps national security decisionmakers and their staffs understand emerging impacts of technology and integrate them effectively into policies through research, teaching, and outreach. CTNSP supports the Department of Defense leadership and Congress while also encouraging whole-of-government and public-private collaboration.

The Defense Horizons series presents original research by members of NDU as well as other scholars and specialists in national security affairs from the United States and abroad. The opinions, conclusions, and recommendations expressed or implied within are those of the contributors and do not necessarily reflect the views of the Defense Department or any other agency of the Federal Government. Visit NDU Press online at www.ndupress.edu.

Linton Wells II
Interim Director, INSS
Director, CTNSP

William T. Eliason
Director
NDU Press