Defense & Technology Paper 84

Task Force Stryker Network-Centric Operations in Afghanistan

Colonel Harry Tunnell

Center for Technology and National Security Policy
National Defense University

Task Force Stryker Network-Centric Operations in Afghanistan

Colonel Harry Tunnell

Center for Technology and National Security Policy
National Defense University

October 2011

This manuscript accompanied the presentation "Military Informatics" given by the author to the Mounted Combat Data Working Group on January 25, 2011, at the National Ground Intelligence Center.

For more information about Intelligence Preparation of the Battlefield with digital technologies, Stryker ACSOPE Decision Maker, and the Battle Command Visualization Suite**,** see the U.S. Army's Center for Army Lessons Learned electronic publication *Smartbook: Guerrilla Hunter Killer,* a Tactics, Techniques, and Procedures series publication.

For more information about Task Force Stryker operations in the Green Zone of Arghandab District, Kandahar Province, Afghanistan**,** see the Joint Base Lewis-McChord Battle Command Training Center video *Operation Opportunity Hold: 5/2 SBCT Operations Enduring Freedom,* Science Application international Corporation (SAIC) contract number DABK01-03-D-0007**.**

The views expressed in this case study are those of the author and do not reflect the official policy or position of the U.S. Army, Department of Defense, or U.S. Government.

Colonel Harry D. Tunnell IV commanded the 5th Brigade, 2nd Infantry Division (Stryker Brigade Combat Team) from January 7, 2007–July 22, 2010; this included a year of combat as the Commander of Task Force Stryker in Afghanistan. A 1984 graduate of the U.S. Military Academy, Colonel Tunnell was commissioned in Infantry and has served in command and staff positions in Mechanized, Light, Air Assault, Airborne, Ranger, and Stryker Infantry units. Colonel Tunnell has served as a combat Infantryman in three campaigns—Operations Just Cause (Panama), Iraqi Freedom (Iraq), and Enduring Freedom (Afghanistan)—and commanded an Airborne Infantry battalion in combat, as well as the Stryker Brigade. Colonel Tunnell has an MA in professional communication studies from Purdue University, an MMAS in history from the U.S. Army Command and General Staff College, an MS in national security strategy with an information strategies concentration from the National War College, and a graduate certificate in human-computer interaction from Indiana University. He has written two books, has published several articles, and is the sole inventor of one U.S patent and one U.S. patent pending.

Defense & Technology Papers are published by the National Defense University Center for Technology and National Security Policy, Fort Lesley J. McNair, Washington, DC. CTNSP publications are available at http://www.ndu.edu/ctnsp/publications.html.

Contents

Introduction

This case study examines the real-world application of the network-centric warfare concept during combat operations in Afghanistan. Network-centric warfare "broadly describes the combination of strategies, emerging tactics, techniques, and procedures, and organizations that a fully or even partially networked force can employ to create a decisive Warfighting advantage."[1] A great deal has been made of the asymmetric advantage of terrorists, insurgents, and guerrillas. In a networked environment with properly trained leaders, soldiers, and units, such advantages are fictional.

Network-centric organizations are supposed to increase their combat power by doing a better job of synchronizing events and their consequences; achieving greater speed of command; and increasing lethality, survivability, and responsiveness of the formation.[2] These capabilities can be a reality in today's operating environment. The main problem with network-centric operations is that there remains a great deal of skepticism among counterinsurgency pundits and others about the concept and the technology necessary to operate in such a fully networked environment.

Task Force Stryker operations in Afghanistan (2009–2010) demonstrate a reality contrary to conventional wisdom. The reality is that *network-centric operations are relevant and effective in the physical, information, cognitive, and social domains of warfare.*[3] Of course, these domains often merge, and it is important to order activities in a way that capitalizes on overlapping capability. For example, the attacks of enemy personnel and their subsequent detention by Afghan National Security Forces described in the vignettes in this paper are obviously in the physical domain. An intersection of domains, however, happens when the movement of forces and positioning of command posts in the physical domain enhances how the cognitive domain informs tactical decisionmaking. The combination of information technology (IT) and sensors creates an extraordinary level of situation awareness and understanding and is obviously in the information domain. However, technology alone is not enough; leaders must properly organize the technology in time and space, which occurs in the physical domain. Furthermore, people must be organized around the technology in ways to improve collaboration, which intersects with the social domain.

> *Several capabilities unique to Task Force Stryker allowed for superior decisionmaking in a networked environment.* ***Stryker ASCOPE[1] Decision Maker*** *is an ArcGIS-based tool that provides geospatial representation of multiple layers of specific information. It is also used for predictive analysis. The* ***Battle Command Visualization Suite*** *fuses intelligence; operations; geospatial data; and governance, reconstruction, and development information for display on Google Earth. The suite is used to show locations and types of captured materials and personnel; identify gaps in intelligence collection; highlight previously unidentified associations among people, terrain, and enemy activity; and visualize battle command information.*

[1] Director, Force Transformation, Office of the Secretary of Defense, *The Implementation of Network-Centric Warfare* (Washington, DC: U.S. Government Printing Office, January 5, 2005), 3.
[2] Ibid, 6.
[3] Ibid, 19–20.

In the cognitive domain, the ability to perform rapid reliable analysis with a variety of tools from the information domain is essential. Because of the wealth of data that is readily available in the digital world, leaders and analysts must understand a commander's intent and critical information requirements to prioritize any data that goes into databases.[4] This "triage" is the only way to prevent organizations from becoming overwhelmed by reams of information and inefficient attempts to catalog it. Despite modern technology, the social domain is independently essential to network-centric operations. A foreign force must have access to important cultural and social information to quickly develop a better situational understanding than an indigenous adversary. Often, the only way to glean such information for database entry is through person-to-person contact by patrols operating in the social domain.

Network Components

A military organization of battalion size or larger has several command posts. The configuration and location of each command post is as important to rapid, reliable communication and network performance as the IT at the command posts. The task forces in this case study are organized around a U.S. Army Stryker Brigade Combat Team and three of its subordinate battalions.

The Army Battle Command System is the automation that is networked together in Army tactical-level command posts. The system includes equipment designed to support maneuver operations, air defense, indirect fire, intelligence, logistics, and the command and control of all basic warfighting functions. The Army Battle Command System is in all U.S. Army tactical brigades.

The 5th Brigade, 2nd Infantry Division (Stryker Brigade Combat Team) was the headquarters for Task Force Stryker. Four command posts were used to execute command and control at the brigade level. Two of the command posts—the tactical operations center (also known as the main command post) and the tactical command post—are part of the typical infrastructure of an Infantry brigade. Two assault command posts, however, were organized, trained, and equipped ad hoc 2 years before the brigade's deployment. The brigade anti-tank company was recapitalized to provide the base infrastructure for the leadership and organization of the two mobile command posts.

The brigade tactical operations center was a fixed facility that had all of the command and control components of the Army Battle Command System. Tactical operations centers are used for command and control, detailed planning, coordination of logistics support operations, and extensive combat information and intelligence research and analysis. Several hundred people were either part of the Task Force Stryker Tactical Operations Center or performed duties in direct support of command post operations.

[4] In recent joint MIT and IBM research, 60 percent of business leaders surveyed believed that their organizations had more data than they could use effectively, and these leaders want to use analytics to take advantage of the wealth of data available to their organizations. See Steve Lavelle, Michael S. Hopkins, Eric Lesser, Rebecca Shockley, and Nina Kruschwitz, *MITSloan Management Review Research Report,* "Analytics: The New Path to Value: How the Smartest Organizations Are Embedding Analytics to Transform Insights Into Action," Fall 2010, 4. The same problem exists for Soldiers. An enormous amount of data is available for leaders at all levels of war—it is necessary to organize people, processes, and systems to take advantage of the extraordinary potential of computers so that the data can be turned into information and then knowledge.

The brigade tactical command post was a smaller version of the tactical operations center. It allowed the Brigade Commander to split command and control for a variety of reasons, including for short durations whenever the Commander wanted to temporarily position in a different location. The tactical command post could also command and control a separate subordinate task force led by the brigade's Deputy Commander. The tactical command post could be deployed for days, weeks, or months and normally had fewer than 100 people. It performed similar day-to-day functions as the tactical operations center but was less capable of detailed operation; logistics; and intelligence planning, coordination, and analysis.

The Task Force Brigade Commander and Deputy Commander each had an assault command post. Each command post consisted of four to six Stryker armored vehicles and had specialized capability as required. Assault command posts allow commanders to personally see the battlefield and include their own individual understanding of the environment in any decisionmaking. Assault command posts are essential because a commander's personal visualization of the battlefield cannot be replicated electronically. Such command posts are highly mobile and can be employed for hours, days, or weeks.

Figure 1. The Task Force Stryker TOC at Kandahar Airfield

The activities of two Infantry battalion task forces and the Brigade Special Troops Battalion (Provisional) are described in the case study. The Infantry units are Task Force Legion (formed from 2nd Battalion, 1st Infantry Regiment) in vignette #1 and Task Force Buffalo (formed from 1st Battalion, 17th Infantry Regiment) in vignette #2. Each task force had a tactical operations center located at a forward operating base. (Battalions have a much smaller version of a brigade main command post.) They also each had a small tactical command post used to establish a static forward command and control node or, because they included enough Strykers, to operate in a vehicle configuration similar to the brigade's assault command post but with far less capability.

The Brigade Special Troops Battalion (Provisional) in vignette #3 consisted of a battalion headquarters, separate companies, D Troop, 8th Squadron, 1st Cavalry Regiment (a specialized military intelligence unit), and other unassigned units operating under the command and control of the brigade. In addition to providing command and control, the battalion led the Governance, Reconstruction, and Development fusion cell on the brigade battle staff. In this capacity, the battalion was responsible for planning and executing population, economic, and governance-focused programs and activities throughout the brigade's area. The benefit of having an organic battalion headquarters in this role is that it ensured any civil-military action was nested within the brigade's approach, meaning all major non-lethal activities—such as development—were fully integrated into maneuver planning. Also, because the brigade operated throughout Regional Command (South), it had the right leadership and staff to conduct effective integration with any of the several national Provincial Reconstruction Teams in the region.[5] The battalion had a main

[5] Several Provincial Reconstruction Teams operated in Regional Command (South): United States, British, Canadian, and Dutch. Having an organic governance, reconstruction, and development component of the brigade

command post and a very small mobile command post comprising Mine Resistant Ambush Protected vehicles and a security detachment. This command post was designed to move military and civilian governance, reconstruction, and development leaders around the battlefield under armored protection independently and without relying on a maneuver battalion for protection.

When the brigade assault command post established a static position for longer than a day, it employed the most critical elements of the Army Battle Command System, as well as a command post node. The assault command post included Secret Voice over Internet Protocol telephones, Secret Internet Protocol Router Network (SIPRNET) access, Microsoft Internet Relay Chat (mIRC), One System Remote Video terminal (OSRVT), individual Land Warrior systems (wearable computers that are digital battle command systems and provide users with location, voice and text communication, and other features), one Land Warrior system configured with a 16-inch screen for command post use, **FM** and tactical satellite (**TACSAT**) radios, a Maneuver Control Station, and Blue Force Tracker and Force **XXI** Battle Command Brigade and Below-Terrestrial. The battalion tactical command post in a vehicle configuration typically included a Remotely Operated Video Enhanced Receiver (ROVER), FM and TACSAT radios, individual Land Warrior systems (and one with a 16-inch screen for command post use), and Blue Force Tracker and Force XXI Battle Command Brigade and Below-Terrestrial.

There are several capabilities unique to Task Force Stryker that allowed for superior decisionmaking in a networked environment. **Stryker ASCOPE[6] Decision Maker** is an ArcGIS-based tool that provides geospatial representation of multiple layers of specific information. It is also used for predictive analysis. The **Battle Command Visualization Suite** fuses intelligence; operations; geospatial data; and governance, reconstruction, and development information for display on Google Earth. The suite is used to show locations and types of captured materials and personnel; identify gaps in intelligence collection; highlight previously unidentified associations among people, terrain, and enemy activity; and visualize battle command information.

Both tools are connected to a database via SIPRNET, but they can operate disconnected with specific layers of pre-loaded information. The ability to conduct rapid analysis of materials and information was a critical part of network-centric operations for Task Force Stryker. The common operating picture displayed for the battle staff in the brigade tactical operations center incorporated components of the Battle Command Visualization Suite by displaying Blue Force Tracker feed, unmanned aerial system (UAS) location data, and operations graphics on Google Earth to show accurate and automatically updated near-real-time locations. This display, which was shown on a large screen, complemented the information on the Maneuver Control Station display next to it. The Command Post of the Future, a desktop workstation, was used to catalog the current status of enemy and friendly activity. (Maneuver Control Station and Command Post of the Future are not unique to Task Force Stryker.)

---

battle staff ensured consistency in focus, coordination, and staff planning within Task Force Stryker and for its subordinate task forces.

[6] ASCOPE is a U.S. Army doctrinal term for Areas, Structures, Capabilities, Organizations, People, and Events. It is a methodology primarily used to examine civil (non-military aspects) terrain. (See Field Manual 3-05.40, *Civil Affairs Operations*, for more on the concept of ASCOPE analysis.)

Task Force Stryker had a one-of-a-kind network configuration. It was networked from Land Warrior-equipped dismounted Infantrymen through mobile and fixed command posts to U.S. Air Force fighter aircraft and UAS. In Task Force Stryker, Land Warrior was integrated with vehicle and aerial systems such as Force XXI Battle Command Brigade and Below-Terrestrial, full-motion video (FMV), and U.S. Air Force Situational Awareness Data Link. (The links between ground and aerial systems are internal innovations.)

Echeloning Command Posts

The actions in this case study center on Arghandab District, Kandahar Province, Afghanistan (the brigade's area of operations was much larger than this district and covered several provinces). From August 2009 to December 2009, the district was the Task Force Stryker main effort, and every battalion in the brigade had a company/battery/troop-size element or larger fighting, or firing into, the area at one time or another. The enemy contacts described in the case study occurred in the agricultural area of the district informally known as the "Green Zone." This Green Zone is to the immediate northwest of Kandahar City and guards several approaches to the city. It is as important tactically as it is agriculturally to southern Afghanistan and Kandahar City. It was a Taliban safe haven when Task Force Stryker arrived in Afghanistan during July 2009, and it had been for several years. Little reliable intelligence was available about the area or the enemy when elements of Task Force Stryker began deploying into the field during the first week of August 2009.

The Task Force Stryker Tactical Operations Center was located at Kandahar Airfield in Kandahar Province. The Task Force Stryker Tactical Command Post was deployed to Qalat, Zabul Province for the first 6 months with the Deputy Commander. This command post later moved to Lashkar Gar, Helmand Province. A four-Stryker vehicle assault command post was with the Deputy Commander at both locations.

The assault command post for the Brigade Commander was located at a Combat Outpost in Arghandab District on the periphery of the Green Zone during vignette #1 and was not deployed during vignette #2. The assault command post moved the Brigade Commander to meetings and key leader engagements to support activities in vignette #3; the Brigade Special Troops Battalion Commander often moved in the assault command post until he was able to establish a separate mobile command post and operate with much greater autonomy.

The Task Force Legion Tactical Command Post in its vehicle configuration was located within a few kilometers of the assault command post on the periphery of the Green Zone during vignette #1. The Task Force Tactical Operations Center was at Forward Operating Base Ramrod in Maiwand District, Kandahar Province.

The Task Force Buffalo Tactical Operations Center was located at Forward Operating Base Frontenac in Shah Wali Kot District, Kandahar Province during vignette #2. A tactical command post was not deployed at the time. The district is to the immediate north of Arghandab District.

The Brigade Special Troops Battalion (Provisional) in vignette #3 had a tactical operations center located next to the brigade main command post on Kandahar Airfield. This battalion did not have a tactical command post, and its mobile command post function was limited to providing armored mobility (it did not need to perform command and control on the move or

from a forward site). This mobile command post was used extensively during vignette #3 to move civil-military leaders, including non-U.S. coalition civilian partners, to the district centers of governance.

There were ten lieutenant colonel-level commands subordinate to Task Force Stryker at the time. The locations of their command posts are not germane to this case study.

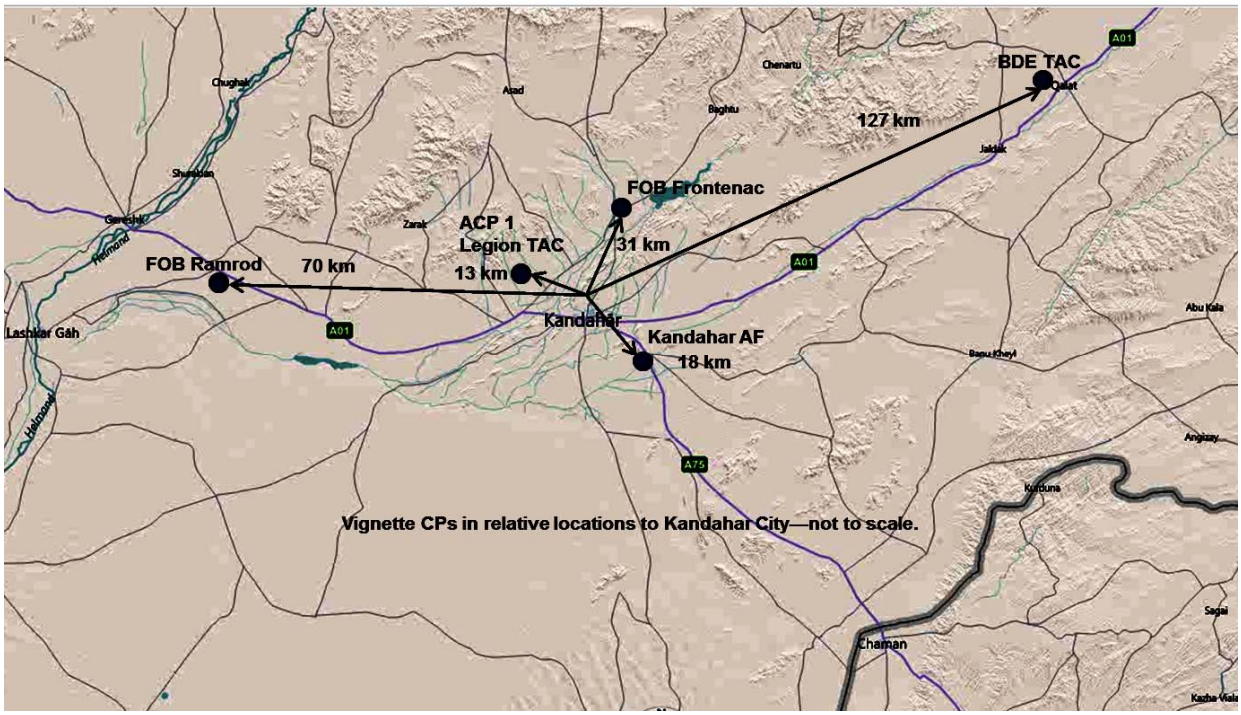

Figure 2. Vignette Task Force Stryker Unit Command Posts

Vignette #1

At the end of August 2009 in Arghandab District, intelligence, surveillance, and reconnaissance (ISR) assets identified people sleeping in fields—an activity normal for the Taliban but not exclusive to it. Based on this suspicious activity, a UAS returned to the area to conduct surveillance on September 1, 2009. Shortly after 7:00 p.m. during this suspicious activity scan, the aerial vehicle operators identified people digging in the center of the road at an intersection. Based on the historically high improvised explosive device (IED) activity in the area, several other indicators, and results of the analysis, the activity was assessed as an imminent threat to local forces.

The Task Force Stryker and Task Force Legion Commanders watched the video downlink of the suspicious activity scan simultaneously at their individual forward-positioned command posts. Task Force Legion executed an aerial attack on the Taliban group at the intersection.

Within a few minutes of the successful attack, several enemy personnel, who had obviously been in overwatch, began to recover remains and equipment from the attack location. Others soon joined them and assisted in the evacuation to a village several kilometers south of the road

intersection. Both Task Force Commanders were able to continuously observe the enemy formation with a variety of ISR as the Taliban moved into a compound. Once the small group reached the compound, 15 or more people joined them—many of whom were obviously armed. At this point, the Task Force Legion Commander began to prepare a request to attack the new target with precision indirect fire munitions.

As the Task Force Stryker command group observed the enemy massing, the Brigade Commander began to review the criteria for engagement in a built-up area with precision munitions; shortly thereafter, the OSRVT operator began saving selected images as directed by the Commander. The Task Force Stryker Assault Command Post communicated via mIRC with the observers controlling the main ISR platform being used to monitor post-strike activity. (Task Force Legion leaders could observe the video feed but did not have SIPRNET and mIRC.) At this point, the observers identified the compound as a possible mosque. When queried by the Task Force Stryker Intelligence Officer, they used mIRC to explain the reasons for their assessment.

The logic used to deduce that the compound was a mosque was reasonable, and the Task Force Stryker Commander terminated planning for an attack with lethal munitions. A swift check of unit locations in Blue Force Tracker and Land Warrior allowed the Task Force Stryker Commander to understand the locations of the closest coalition force. In conjunction with the Task Force Legion Commander, the readiness of and partnership status with Afghan Security Forces was quickly assessed—there was a partnered Task Force Legion company close enough to respond. The Task Force Legion Tactical Command Post digitally marked the compound's location in Land Warrior and other systems, and the company deployed to conduct a tactical callout. (Tactical callouts are a specialized form of cordon and search.)

After the partnered company arrived and conducted the tactical callout, it learned that the compound was in fact a mosque and that the enemy had used this location as a transition point when evacuating casualties after the aerial attack. The partnered unit immediately began to conduct consequence management and defensive information operations on site with local elders.[7] Meanwhile, the Task Force Stryker Assault Command Post, located at an Afghan National Army Combat Outpost, was informed by one of the Afghan unit's Canadian mentors that its liaison at the Arghandab District Center reported that four very seriously injured men had shown up at the district center shortly after 9:00 p.m. requesting medical aid. (Afghan National Security Forces and mentors were part of the ongoing operation by Task Force Stryker.) The men were enemies who were wounded in the attack, and the assault command post ordered the battle staff at the brigade tactical operations center to request that Afghan Security Forces follow the enemy combatants through the medical process and determine final disposition for them post-recovery.

Throughout the almost 2 weeks of assault command post operations, the Task Force Stryker Intelligence Officer and Assault Command Post Battle Captain updated the brigade's digital common operating picture using the Maneuver Control Station. After adjusting the common

[7] U.S. Army information operations doctrine makes a provision for offensive and defensive information operations. Defensive information operations are designed to preserve decisionmaking capability. Relationships with civilian communities and local, district, and provincial government officials were considered enabling operations by the Task Force Stryker Commander and thus essential to maintaining task force and small unit freedom of maneuver.

operating picture, the information was sent electronically to the Task Force Stryker Tactical Operations Center, and the **main command post** then distributed it electronically to other task force command posts as needed. This distribution ensured the Task Force Stryker elements throughout Kandahar and Zabul Provinces had the same updated tactical assessments as the command group located at the forward-positioned mobile command post.

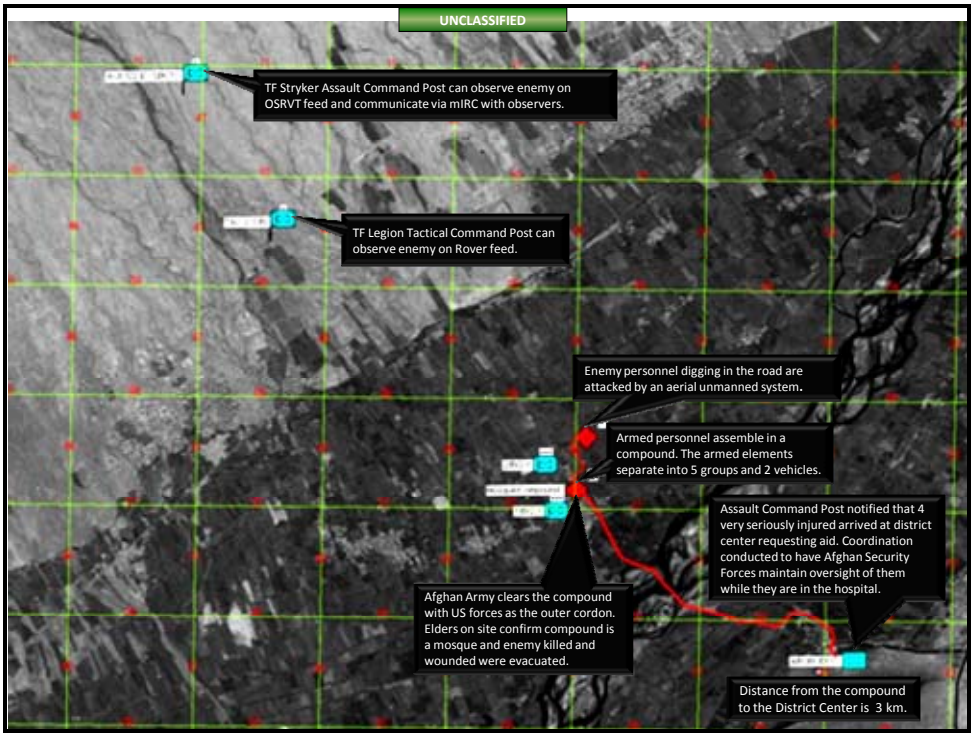

Figure 3. Screen Capture, September 1, 2009 (Notes Added by Author)

Vignette #2

Shortly after 7:30 p.m. on September 23, 2009, an intelligence report indicated that a large body of Taliban personnel was maneuvering within Arghandab District. The Task Force Stryker Tactical Operations Center received the report. The information was assessed as being reliable enough for action, and Task Force Buffalo, the unit responsible for ground tactical operations in the suspected area of Taliban activity, was notified. The battle staff at the brigade main command post coordinated with Regional Command (South) for ISR. A UAS with FMV was re-tasked to support Task Force Stryker.

The FMV capability was used to identify a suspected enemy formation at a grape hut in a rural agricultural area of the district. Task Force Buffalo was allocated rotary wing aviation to further develop the situation. The Task Force Buffalo command group and the aviation element worked closely together to positively identify the group and coordinate activity. After identifying weapons and other activity consistent with a Taliban formation, an attack was conducted. In addition to the enemy casualties, numerous secondary explosions were observed.

As the attack commenced, the Task Force Stryker battle staff conducted a predictive analysis of the enemy response to being attacked. Taliban members were known to seek out quality medical

care when wounded (see vignette #1). To support a "military estimate of the situation," members of the brigade staff had developed a unique tool known as Stryker ASCOPE Decision Maker.

Using Stryker ASCOPE Decision Maker, the Brigade Intelligence Officer identified four possible facilities the enemy was likely to use to treat the wounded. Stryker ASCOPE Decision Maker affords easy access to the metadata behind each layer of information. The Battle Captain at the brigade tactical operations center emailed the relevant amplifying data about each location (such as grid coordinates and history of interaction with the Taliban) to liaison officers, who passed the information to coalition partners and Afghan National Security Forces.

By midnight on September 23, 2009, Afghan National Police had identified six enemy personnel who were admitted to the first facility assessed as a likely evacuation site. Afghan National Security Forces agreed to take responsibility for the enemy fighters as they progressed through the medical system.

Immediately after the engagement, the brigade Information Operations Officer began a defensive information operations action that outlined the need to attack Taliban. The next day, Taliban messaging falsely claimed that innocent farmers had been attacked. By 5:00 p.m. on September 24, 2009, Kandahar provincial leadership released radio messages reinforcing the fact that the men were Taliban and that coalition operations were appropriate.

Taliban messaging ceased, and Afghan National Security Forces monitored the wounded at the hospital until a further indigenous determination as to their disposition could be made. The Task Force Stryker Commander coordinated with the Aviation Task Force Commander for permission to use the attack video as part of the defensive information operations plan. Several days later, the Task Force Stryker Commander personally showed a sanitized version of the attack video to the provincial leaders, who had authorized the public messages in support of coalition operations. This messaging was done as a defensive information operations measure to maintain the credibility of Task Force Stryker with civilian indigenous leaders. The local community in Arghandab District and the surrounding areas continued to support Task Force Stryker operations in the area and eventually began reporting IED and cache locations to Task Force Buffalo and Afghan National Security Forces. (This note does not imply that the attack was the catalyst for reporting, but it does indicate that the months of intense fighting by Task Force Buffalo and other members of Task Force Stryker to secure the area actually created bonding with the local population and the Task Force Stryker brand.)

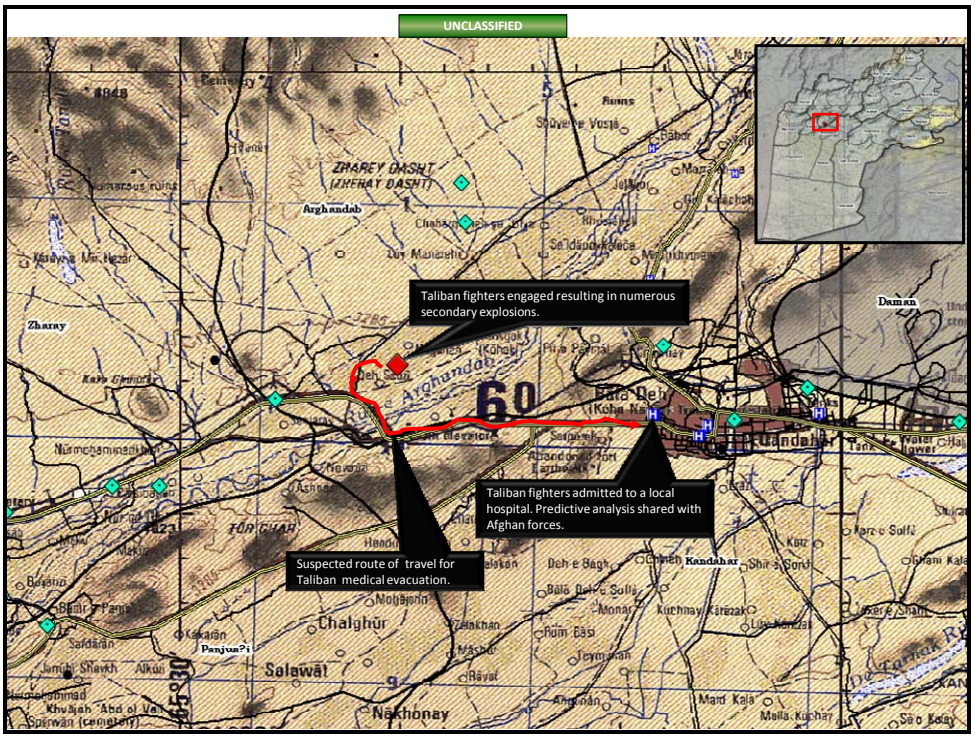

Figure 4. Stryker ASCOPE Decision Maker Hospital Layer Screen Capture

Vignette #3

As the maneuver operations were ongoing in Arghandab District, the Brigade Special Troops Battalion (Provisional) simultaneously began planning for comprehensive governance, reconstruction, and development activities in the district. The goals for development exceeded the brigade's capability, so brigade leaders approached several outside agencies for help. Almost every organization insisted the security situation remained too volatile for it to conduct activities. The Office of Transition Initiatives (OTI) also voiced reservations but agreed to position OTI officers at the Arghandab District Center. This effort became essential to the realization of a model for district governance and contributed substantially to networking in the social domain. To promote a better understanding of the situation and the pace of security operations, the Brigade Special Troops Battalion leaders in their governance, reconstruction, and development capacity deployed Stryker ASCOPE Decision Maker during a series of key leader engagements as a visual demonstration of the rapid security successes of Task Force Stryker.

Beginning in August 2009, Task Force Stryker's Governance, Reconstruction, and Development fusion cell began a series of key leader engagements with U.S. Agency for International Development (USAID) leaders to operate in the district. USAID officers were concerned that the security situation would not provide the freedom of movement necessary for USAID implementing partners to conduct successful development activities and that the district shura (a traditional form of local governance by tribal elders) was not representative of the district's population.

By October 2009, security and representative governance had improved, and Task Force Stryker used the Stryker ASCOPE Decision Maker to overlay historical significant activities (SIGACTS) data. The tool demonstrated a substantial decline in enemy action over time, showed agriculture data and the potential for expansion, visualized the force lay down of coalition forces and Afghan National Security Forces, and highlighted that village elders were attending the district development shuras (representing about 80 percent of the district). All of this was done to demonstrate that the east side of the Arghandab River was ready for USAID programs. By late October 2009, USAID agreed to implement Afghanistan Voucher for Increased Production of Agriculture Plus (AVIPA Plus) in the district—a $270 million program aimed at improving Afghanistan's licit agriculture. The accurate, comprehensive, and timely visual representation had helped convince USAID leaders to develop this former Taliban stronghold. On November 5, 2009, Kandahar Provincial Governor Tooryalai Wesa announced at the Arghandab District Center that the district had been selected as the first location in the province for AVIPA Plus. By December 2009, the program was in the district and operating inside the Task Force Buffalo persistent security bubble.

The Canadian signature project to rehabilitate the Dahla Dam and the corresponding irrigation networks south of the dam was scheduled to begin during the winter of 2009–2010. The project stretches from Shah Wali Kot District south through Arghandab, into Kandahar City, and further south into Dand District. Because of security concerns from a security assessment conducted in January 2009, the project's security manager voiced reservations about beginning work in Arghandab. The project leaders indicated that they would only work in Dand and Kandahar City and would delay work in Arghandab for another year.

Arghandab has been the home district of the Alikozai tribe since the mid-1700s. In the past few years, the area had seen support for the Government of the Islamic Republic of Afghanistan steadily wane and support for the Taliban increase. Alikozai tribal leadership indicated they felt disenfranchised because they watched the Popalzai and Barakzai tribes accrue tremendous wealth from coalition contracts and development while the Alikozai tribe received little. It became apparent that if the Canadians began work in only Dand and Kandahar City, areas of significant Popalzai and Barakzai populations, the Alikozai population in Arghandab would once again see this negative dynamic at work.

Task Force Stryker again deployed Stryker ASCOPE Decision Maker as part of the key leader engagement process, along with Battle Command Visualization Suite-derived threat assessments. Task Force Stryker intelligence staff shared the information about the Alikozai tribe with Canadian representatives and urged them to support activities in Task Force Stryker areas. On December 3, 2009, a team from Task Force Kandahar and the Kandahar Provincial Reconstruction Team (both Canadian) promised elders at a local development shura that they would begin work in Arghandab in January 2010. The network-centric approach was a major factor of these successful key leader engagements.

Specifically, in Arghandab District, AVIPA Plus had multiple ongoing cash-for-work projects with more than 7,000 local men working and millions of dollars planned for agriculture training, vouchers, and small grants in the district throughout 2010.[8] The program would successfully expand beyond the eastern side of the Green Zone. Furthermore, substantial development occurred throughout the remainder of the Task Force Stryker area, much of which was informed by the network-centric decisionmaking tools using different layers of information. Network-centric operations that discover knowledge were central to the ability of the task force and its subordinate units to develop the level of understanding necessary to pursue objectives that support maneuver, create licit wealth for Afghans, and improve governance. Regardless of the confidence of military leaders, development personnel must be convinced that adequate persistent security will be available to minimize risk for their personnel before they will consider operating in contested areas. The tools that are common in Task Force Stryker's network-centric paradigm are particularly well suited in that regard and have proven effective many times.

> *"Subsequent data mining indicated a reason for the elder's recalcitrance; he had a long association with the Taliban. Such an assessment would have been unlikely using legacy processes—but it took merely a matter of minutes of visualization to generate new requests for information and collection priorities that yielded important results."*

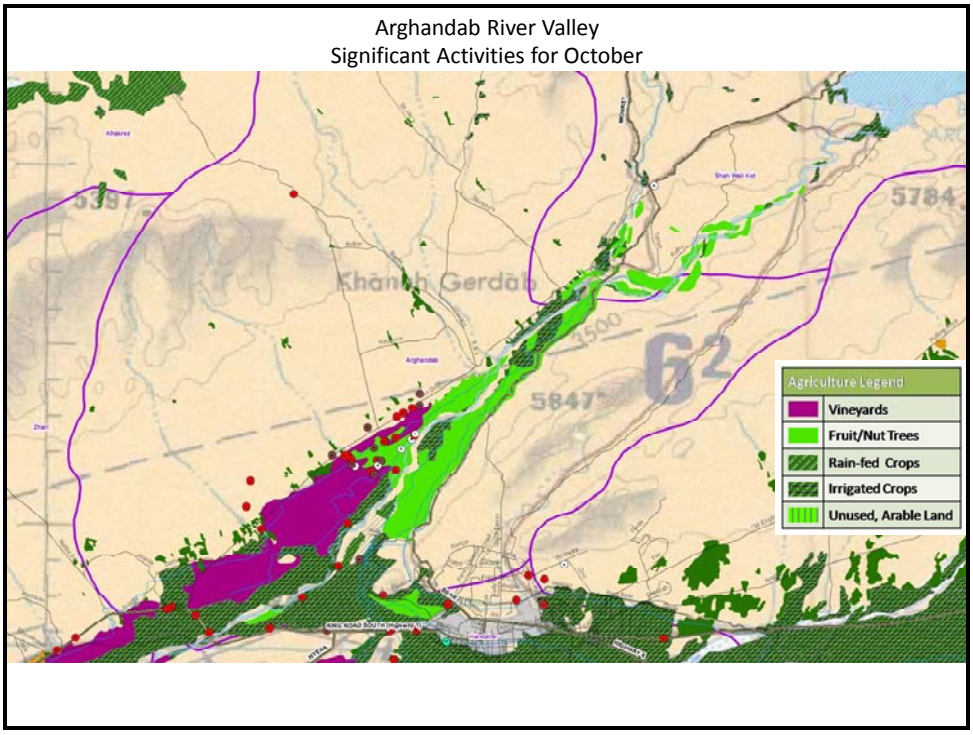

Figure 5. Type of Layer Used to Demonstrate the Success of Security Operations (Red Dots are Enemy Contact—Note Their Absence in the East)

[8] Afghanistan Vouchers for Increased Production of Agriculture Plus Program Weekly Activity Report, International Relief and Development, February 1, 2010, 6.

Lessons Learned

Stryker ASCOPE Decision Maker, Battle Command Visualization Suite, and similar tools help develop rapid, effective situational understanding. True network-centric operations are far more than merely improved situational awareness—they include a level of understanding that can only be gained through disciplined research and analysis. Using computers to collect, store, manipulate, and transform data, entering relevant but nontraditional information into a tactical database, and ensuring information is properly represented, searchable, retrievable, and available on short notice are all part of the network. Computers today can be used to discover and share knowledge throughout a formation much more rapidly than any previous technology at any other time in military history.

Databases can take a substantial amount of time to develop; it took 10 months for the potential of the initial Stryker ASCOPE Decision Maker database to be even partially clear. The Distributed Ground Common System—Army known as **DCGS-A** (pronounced *"D-Sigs-A"*), which is the intelligence component of the Army Battle Command System, has the potential to be a powerful capability once the database matures. (DCGS-A includes the same ArcGIS capability as Stryker ASCOPE Decision Maker, so they can share data.) The fact that other data sources, such as patrol reports, key leader engagements, **CIDNE**, TIGRNet, and Marine Link, can be ingested into DCGS-A allowed the brigade to incorporate local data from other units whenever it moved to an unfamiliar area. Furthermore, an important feature of the visualization capability of these tools is the metadata behind any icon. The metadata itself is generally classified, so the actual visualization can be designed to convey information at a secret or unclassified level based on the audience. (One caution is that the arrangement of icons on any visualization can convey information about maneuver, resources, processes, and other procedures that one may want to keep secret.) Generally speaking, using these tools, important information can be shared with a variety of audiences. For example, screen captures could be included in this case study because the visualization is unclassified even though the metadata, which is not part of the case study, may have included sensitive information.

It is important to note that these tools are also used to conduct nontraditional analysis in support of military decisionmaking. For example, Stryker ASCOPE Decision Maker was used to conduct a detailed analysis on unused arable land to determine if population centers in this agricultural-based region of Arghandab District had the potential to expand *away* from areas susceptible to Taliban influence. The analysis determined that the potential did exist and thus development resources could be applied at these locations with a greater chance of success. (See the long southwest-northeast running red line to the west of the Green Zone in Figure 6 for the road assessment; the hatched area is unused arable land.) These tools can also conduct financial forensic analysis, and suspected locations of criminal activity have been layered and combined with Taliban activity layers to analyze potential criminal activity and Taliban guerrilla activity.

The Battle Command Visualization Suite has been used to simultaneously display enemy infiltration routes, village locations, elders associated with each village, and the level of participation of each elder in district governance. For example, it was discovered that a few Taliban infiltration routes terminated at the village of an elder who refused to participate in local governance. This curiosity generated new intelligence requirements. Subsequent data mining indicated a reason for the elder's recalcitrance; he had a long association with the Taliban. Such

an assessment would have been unlikely using legacy processes—but it took merely a matter of minutes of visualization to generate new requests for information and collection priorities that yielded important results.

In such an information-rich environment, it is essential to have disciplined processes to ensure unnecessary information is not entered into a database, ensure quality control mechanisms are in place, limit redundant data basing, and develop agreements with adjacent organizations so information efforts are complementary. Compatible tools make data collection, representation, storage, and retrieval much easier. The geospatial section of the brigade battle staff collected information about infrastructure, past projects, agriculture, tribes, patrol data about local sources of instability, and other topics. The Brigade Special Troops Battalion (Provisional) collected key leader engagement data, identified illegal checkpoints on highways, and conducted financial forensics. The Intelligence and Operations sections contributed traditional military information.

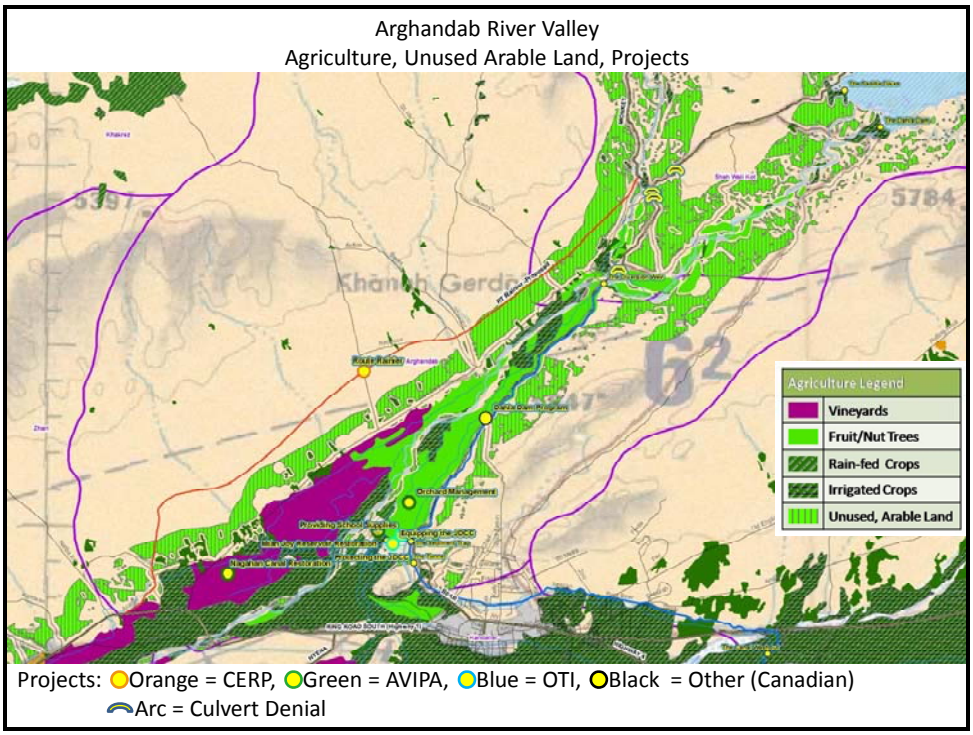

Figure 6. Stryker ASCOPE Decision Maker Layer Showing Development Information

Because all organic battalions within the brigade used a combination of ArcGIS and Google Earth, it was easy to share files down to the battalion level. Innovations such as ingesting Blue Force Tracker and FMV data into Google Earth meant that near-real-time locations were included in brigade analysis and visualization. Standardization made the information shareable and searchable; because each section inevitably focused on its own area of expertise, the overall enterprise benefited from better quality and greater potential. For example, the geospatial section collected more than 800 layers of information, and the intelligence section ingested nearly 50 data sources. Even with all of the information available on DCGS-A, the Intelligence Officer used the geospatial section's hospital layer for predictive analysis in vignette #2. The brigade eventually fielded Palantir, a powerful, sophisticated, and easy-to-use software that extended a substantial part of the network's knowledge discovery capability to the company level. (The

battalion headquarters should conduct quality control of company-level inputs, while the brigade headquarters should do the same for battalion contributions. Once brigade-level quality control is completed, the information can then be incorporated into the larger enterprise for Afghanistan.)

The combination of Afghan National Security Forces' immediate involvement to positively identify and control wounded Taliban combatants, rapid defensive information operations, and official government radio announcements overwhelmed Taliban attempts at negative word-of-mouth messaging. Subsequently, leadership's employment of technology to improve Afghan government officials' understanding of the reliability and precision of American military capability created further bonding between indigenous and Task Force Stryker leaders.

To capture a fleeing enemy, soldiers may have to conduct risky pursuits that can draw them into IED-laden areas or have to search civilian compounds and homes at night. The network-centric operations described herein, however, resulted in the identification of several wounded enemies without exposing a single American, coalition, or Afghan soldier to unnecessary danger. The result was lower risk for coalition forces, prevention of opportunities for collateral damage, and prediction of enemy action in a timely enough manner to act.

Normally, if enemy combatants are not detained at the immediate area of contact after an operation, their status is usually unknown unless subsequent intelligence reporting becomes available. Information from such reports is usually days, weeks, or months old and too late for small unit action. Network-centric operations allow a headquarters to capture and analyze combat information promptly and share it with subordinate units that can act on it.

Mixes of mobile and fixed command posts are important to establishing a reliable network. This blend of facilities ensures fixed sites can conduct detailed analysis and coordination quickly with a robust battle staff and ensures agile mobile command posts can provide fast, accurate updates. The fixed command posts are also responsible for disseminating new information throughout the entire command and control enterprise. Finally, smaller mobile command posts allow leaders to position themselves at critical points of decision so they can adequately and simultaneously operate in the physical, information, cognitive, and social domains of warfare.

Command posts must be positioned in the correct place to improve information sharing. The ability to share information between Canadian mentors and Task Force Stryker members was in the social domain of warfare. Not only was the command post located properly but also all of the Canadian mentor teams in the area had substantial details about American task force operations in their area. This knowledge allowed them to assess whether information was relevant and then bring it to task force leaders.

The combat information gleaned through the network and turned into intelligence by the brigade informed future Intelligence Preparation of the Battlefield. (Unlike most brigades that are limited to reporting combat information, Stryker Brigade Combat Teams have enough analytical capability to report intelligence.) Before the deployment, the Intelligence Community could answer very little of the brigade's Taliban order of battle information requests. The information gleaned through the network in the first month (including analysis of reporting from adjacent units) indicated that enemy strength exceeded estimates substantially in some areas and that the enemy operated in guerrilla formations rather than small IED teams. This Taliban held terrain, conducted overwatch, massed, and could rapidly disperse, which is contrary to the conventional

wisdom of small IED networks. The enemy employed IEDs as part of an overall tactical framework much like conventional formations employ minefields and point obstacles.

Social and human terrain are incorporated into the network. This information became important as the enemy formations were degraded and the enemy attempted to operate more among the population. The enemy was eventually defeated in the Green Zone in the near term as the population and government officials bonded with the Task Force Stryker brand.

It would be a gross overstatement to imply that all of the network-centric tools and command, control, communications, and computers worked perfectly all of the time and achieved a 100-percent success rate in tactical operations; intelligence; governance, reconstruction, and development; or any other activity in Task Force Stryker areas. It is not, however, an exaggeration to state that these network components were used routinely, performed reliably, and improved the capability of the brigade substantially. A significant amount of combat occurred because the task force was required to go into areas absent sustained coalition presence, frequently infested with Taliban, and considered not permissive by coalition leaders, provincial officials, and local Afghans. (Task Force Stryker units operated primarily but not exclusively in Zabul, Kandahar, and Helmand Provinces.) However, physical and human terrain were secured in many of these areas, and development was initiated. Without applying the concept of network-centric operations and having the tools and training to implement it, such little collateral damage and such rapid results would not have been possible.

Conclusion

In the Task Force Stryker experience, it is true that a robustly networked force improves information sharing. Information sharing improves the quality of information and shared situational awareness. Shared situational awareness improves collaboration and self-synchronization and enhances sustainability and speed of command. All of these, in turn, dramatically improve mission effectiveness.[9] The aspects of network-centric operations clearly have value in today's operating environment. The basic warfighting concepts for battle command still apply—leaders have to be able to communicate, they have to position themselves properly on the battlefield, and they have to be able to provide necessary resources to subordinate units.

The unrealized benefit of network-centric operations in the U.S. military rests in the enhanced speed and quality of decisionmaking that the technology *already available* in the Department of Defense can facilitate. Rather than fear asymmetric foes, it should be the goal of a networked force to have such a substantial advantage during combat that the enemy is the one hampered by his asymmetric approach to maneuver, population engagement, and information operations.

Network-centric operations can be viewed as a form of mass[10]—although different than the type of mass commonly thought of with maneuver elements. One of the benefits of using Arghandab District in the case study is that it demonstrates that network-centric operations can influence

[9] The tenets and principles of network-centric operations are paraphrased from Director, Force Transformation, *Network-Centric Warfare*, 7.

[10] Mass is a military term of art commonly used to describe the grouping of resources or activities together in a way to increase lethality—it is normally done in the physical domain. Massing maneuver formations on an enemy or massing the fires of a capability, such as artillery, are common examples.

everything in the environment, including populations, formations, supply chains, terrain, and government institutions. The improved operations in turn influence bonding among the network-centric force, the population, government leaders, and Afghan National Security Forces. When concentrated in a geographic area, on specific aspects of human terrain, or on particular warfighting functions, network-centric operations can achieve a form of mass.

Figure 7. Assault Command Post Patrol Through Kandahar City

The combination of fires, maneuver, and liaison on small enemy formations in vignettes #1 and #2 enabled by network-centric operations parallels the traditional concept of mass. In vignette #3, however, it is noteworthy that the massing of the network to support the cognitive and social realms of war, while not typical, is nonetheless effective. The fact that Arghandab District was the brigade's main effort is important to the notion of mass in network-centric operations. A battalion conducts digitally enhanced command and control—it does not control or manage all aspects of the network or have access to all of the available robust decisionmaking aids during the military decisionmaking process. The brigade combat team is the first echelon in which there are enough resources that a commander organizes to achieve true network-centric *battle command*. The designation of a brigade main effort means that the network is, in effect, massed to achieve a specific objective.

Network-centric warfare allows units to have an overwhelming, cascading effect on an adversary that causes his collapse and subsequent defeat. This effect is especially possible in an operating environment heavily populated by noncombatants because the wealth of cultural and social data that is available, when properly databased, is more readily obtainable and hence *usable* by a networked force than by an enemy who only has the information in his head. The confidence and improved performance brought by effective networking mitigates the cultural and social advantages that today's illiterate, ill-equipped indigenous adversary is routinely credited with having.