AU/ACSC/TEAGUE/AY09

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

INFORMATION SHARING CHALLENGES IN A COALITION ENVIRONMENT

by

James C. Teague, MAJ, USA

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisors: Lt Col Lance Mathews and Maj Joseph Dene

Maxwell Air Force Base, Alabama

April 2009

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
APR 2009	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Information Sharing Challenges in a Coalition Environment	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) **Air Command And Staff College Air University Maxwell Air Force Base, Alabama**	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
The original document contains color images.

14. ABSTRACT

The United States has been involved in the conflicts in Afghanistan and Iraq since 2001 and 2003 respectively. Since entering these conflicts the United States has worked with other countries as part of a coalition. Internally, the United States military has realized an evolution with the capability to transmit, store, analyze, and manipulate data supporting these operations. Situational awareness tools, intelligence gathering technologies, and battle command systems have enabled military commanders to dominate on the information battlefield. New tools allow commanders to collaborate, plan, and assess operations on a global scale. Video teleconferencing brings our leaders together regardless of location. Internally, the United States has a digital capability that extends beyond any of the partners fighting in the coalition. The large disparity in capabilities among coalition partners creates gaps in information exchange. How are our commanders dealing with these gaps in information exchange? How can they achieve unity of effort if they cannot share information because of security policies and regulations and the use of U.S. only systems? These questions will be addressed in this research paper. Reviews of available literature, guidance, regulations, and interviews will serve to frame the problem, provide analysis, and provide recommendations to mitigate the challenges of information sharing in a coalition environment.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**40**	

Disclaimer

Contents

Page

Abstract

The United States has been involved in the conflicts in Afghanistan and Iraq since 2001 and 2003 respectively. Since entering these conflicts the United States has worked with other countries as part of a coalition. Internally, the United States military has realized an evolution with the capability to transmit, store, analyze, and manipulate data supporting these operations. Situational awareness tools, intelligence gathering technologies, and battle command systems have enabled military commanders to dominate on the information battlefield. New tools allow commanders to collaborate, plan, and assess operations on a global scale. Video teleconferencing brings our leaders together regardless of location. Internally, the United States has a digital capability that extends beyond any of the partners fighting in the coalition. The large disparity in capabilities among coalition partners creates gaps in information exchange. How are our commanders dealing with these gaps in information exchange? How can they achieve unity of effort if they cannot share information because of security policies and regulations and the use of U.S. only systems? These questions will be addressed in this research paper. Reviews of available literature, guidance, regulations, and interviews will serve to frame the problem, provide analysis, and provide recommendations to mitigate the challenges of information sharing in a coalition environment.

Transforming to a network centric force requires fundamental changes in processes, policy, and culture.

John G. Grimes, DoD Chief Information Officer

INTRODUCTION

The past decade has been a revolution in our ability to access, store, analyze, and manipulate information. This revolution in information technology is, in large part, due to the proliferation of the internet and the variety of tools used to access it. This network of computers, telephones, and other devices has changed every aspect of our lives. From the entertainment industry to the corporate world, the internet has made access to products, services, and information available to anyone with a computer. The speed with which this new domain provides information continues to accelerate and has played a pivotal role in enabling our global economy and society.

As significant a role this new domain has played in the private sector, it has also changed the way our military prosecutes combat operations. The demand to transmit more data at faster speeds has seen dramatic increases. This demand for information has increased tremendously as new battle command systems have been developed and commander's information requirements increase. To get an idea how significant this change is one simply needs to compare the requirements of bandwidth from Operation Desert Shield/Storm and Operation Iraqi Freedom. Operation Desert Shield/Storm required approximately 47 megabytes of bandwidth compared to approximately 10 gigabytes for current operations across the entire Iraqi operational area.[1] Having the capability to pass information across the modern battlefield instantly provides commanders the ability to achieve information superiority over an enemy. Information superiority is the ability to gain situational awareness of friendly and enemy forces, exchange relevant information, and make

decisions quicker than the enemy.[2] Achieving information superiority facilitates unity of effort thus quickly meeting military objectives and, ideally, ending conflicts.

This new global environment requires nations to develop coalitions when considering the implementation of the military. Operating within a coalition makes it difficult to achieve unity of command. It is possible to achieve unity of effort without unity of command. When achieving unity of command is not possible, or feasible, coalitions must achieve unity of effort. That is, every partner within a coalition should be focused on a single goal. It is this unity of effort that makes coalitions successful in achieving military objectives and quickly terminating conflicts with a desired outcome.

Coalitions are developed with nations having similar interests and objectives; however, these partners may not maintain similar technical capabilities. When one nation has a significantly greater capability to gather, process, and transmit information but refuses or fails to share the information how can the coalition achieve unity of effort? The United States finds itself in a position of information technology dominance and its application in military operations. If the United States were in a position to share information with all its coalition partners how much more efficient would the coalition be? How is unity of effort being achieved if restrictive information sharing policies are in place? What challenges are being faced by commanders in the field due to information sharing restrictions? What solutions are available to ensure relevant information can be shared among coalition partners without compromising national security? These questions are the basis for this paper. It will attempt to provide answers to these questions, show how commanders are currently sharing information in the coalition environment, and offer feasible

recommendations for future operations. The focus of this research will primarily be at the tactical level of war but can be applied to the operational and strategic levels as well.

DEFINITIONS

When discussing a topic such as information sharing a few common definitions are required. Definitions for the terms collaboration, data, domains, information sharing and networks is required for commonality. Collaboration is a "pattern of interaction where two or more parties are working together toward a common purpose."[3] Data is "representation of facts, concepts or instructions in a formalized manner suitable for communication, interpretation or processing by humans or automatic means."[4] Domains are "a sphere of activity, concern, or function."[5] Information sharing is "making information available to participants (people, processes, or systems). Information sharing includes the cultural, managerial, and technical behaviors by which one participant leverages information held or created by another participant."[6] Networks are "a complex, interconnected group or system. These networks include social, information technology, and communications networks."[7]

BACKGROUND

The Technological Revolution

Technology continues to change at an astounding rate. Anyone with a computer has realized how quickly technology changes as the new computer they purchased quickly becomes obsolete in a few short months. The same thing has occurred with technology supporting military operations. The best way to show how technology has changed is to trace its evolution through the

career of an officer who has commanded in combat at multiple levels. Colonel Stephen Twitty is a U.S. Army infantry officer who has commanded soldiers at the company, battalion, and most recently brigade combat team level. Each of these commands involved combat operations beginning with Operation Desert Shield and Operation Desert Storm, the initial invasion of Iraq in 2003, and ending with an extended rotation to Northern Iraq from October 2006 to January 2007. Colonel Twitty has reaped the benefit of the technological revolution through an evolving command and control capability. In an interview with Colonel Twitty he discussed his experience with command and control tools used in each of the combat operations he was involved in as a commander. As an overview, this evolution in command and control tools will be reviewed using Operations Desert Storm, Operation Iraqi Freedom I, and Operation Iraqi Freedom VI.

As a young company commander Twitty found himself preparing his unit to deploy to Kuwait in 1990. His company was part of the United States' mission to push the Iraqi Army from Kuwait and re-establish national boundaries. He indicated tools available to commanders during this operation to execute battle command were very basic by today's standards. At the lower echelons, where Twitty worked, there were no communications systems available to extend over distances more than 30 kilometers. The FM radio was the primary command and control tool available but the distribution numbers of these radios was not what it is in today's military. The most sophisticated intelligence, surveillance, and reconnaissance (ISR) tools available were pilots in helicopters operating hand held video cameras. These videos could not be transmitted across the battlefield, they were sent using couriers. The battalion level headquarters had a similar compliment of these basic tools but were sometimes augmented by a single long range radio.[8]

Fast forward one decade and Twitty once again found himself preparing his soldiers for deployment to Iraq. This time it would be an all out assault with a mission focused on changing the regime in power. Twitty commanded an infantry battalion within the 3rd Infantry Division. Although the FM radio remained the primary means to execute battle command, other tools were introduced that enhanced situational awareness. COL Twitty stated the introduction of Blue Force Tracker (BFT) (see appendix A) allowed him to see friendly forces, enemy forces, display graphics, transmit detailed orders, and share information. Because of the nature of BFT's transmission medium all of this could be done at extended distances. This new technology provided commanders at the lowest tactical levels a reliable communications link spanning the entire theater. The United States military had gained information superiority by introducing this and other similar tools to tactical formations prosecuting the war.[9]

The quest for information continued through Operation Iraqi Freedom and as the United States entered a counter-insurgent fight in Iraq, commanders recognized how important it would become to dominate the information war. Information sharing would be critical to defeating the insurgency in Iraq. COL Twitty, once again, found himself in command of a unit preparing to deploy to Iraq. In his third deployment to Iraq, COL Twitty would serve as Commander, 4th Brigade Combat Team (BCT), 1st Cavalry Division. His new unit was the newest BCT fielded through the transformation of the Army. This new BCT was one of the "digitized" forces which fielded information systems that were previously only seen at the highest levels of the military. Capabilities included video teleconferencing, streaming video by unmanned aerial vehicles, secure and non-secure voice over internet protocol (VOIP) telephones, satellite telephones, BFT, and computer systems that received real time updates from every combat vehicle on the battle field.

The commander's ability to gather information was tremendous. This capability did not only exist at the BCT level. Many of these capabilities were pushed to the battalion and company level as well. The ability to receive, analyze, store, and transmit information reached a pinnacle of modern warfare with the introduction of these new tools.

Over a decade COL Twitty realized a significant evolution in battle command systems focused on information superiority. With the introduction of each new technology the commander's ability to see themselves, see the enemy, and make timely decisions on the battlefield was enhanced. With all of this new capability COL Twitty warned, though, the technological gap between U.S. forces and coalition forces, the Iraqi Security Force in this case, makes much of this capability useless when sharing information among these partners. The technology available to commanders today certainly enhances their ability to execute battle command but if coalition partners have no commonality, information sharing is left to face-to-face meetings, cultural understanding, mutual trust, and friendships. COL Twitty was tied to none of these technological innovations and felt the best way to execute battle command, gain situational awareness, and share information with coalition partners was to get out and meet with leaders on the battlefield. Providing information to Iraqi leaders helped him create trust which resulted in bonds being formed and actionable intelligence being shared which aided both forces during combat operations.[10] In fact, when speaking with COL Twitty's operations officer, Lieutenant Colonel Jeff Stewart, he admitted the biggest challenge with information was being overwhelmed. Often, LTC Stewart said, there was so much information coming in through these sources it was difficult to analyze it and determine what was important and needed to get briefed to the

commander.[11] This evolution in technology has certainly facilitated decision making within the U.S. military; however, it fails to do much to facilitate information sharing with coalition partners.

Information Sharing Success Story

There are many information sharing success stories from current operations in Iraq and Afghanistan, across all of the services. Many of these examples of successful information sharing are contained in the Department of Defense Information Management & Information Technology Strategic Plan 2008-2009. This document highlights many of the objectives for information technology and uses these examples of information sharing as proof that the sharing of information can save lives. One particular example is that of the First Cavalry Division who has served in Iraq on several occasions and is currently in theater as this is written. The following is one particular example of information sharing in action.

> CavNet was designed as a web-based interactive community to help officers in the 1st Cavalry Division in Iraq trade information at the tactical level about insurgent tactics, gear and even advice on running effective civil affairs operations. In one case, it was learned that insurgents were booby-trapping posters of Moqtada al-Sadr- the Shiite cleric. When the posters were ripped down, an Improvised Explosive Device (IED) would detonate. This information was posted to CavNet. Another officer, operating in another sector of Baghdad, read about this new tactic on CavNet and briefed his men about this new technique. Later that day, using this information, soldiers were able to spot these booby traps and disarm the IEDs without any casualties. Without CavNet there was no way that this type of tactical information could be disseminated quickly and efficiently.[12]

These types of tactical successes highlight the desperate need for standardized tools to share information. The sharing of information has directly impacted our soldier's survivability on the battlefield. This example is only one instance of many that have saved American lives. The type of information sharing depicted in the First Cavalry Division scenario is an example of

knowledge management. Knowledge management is the systematic process of discovering, selecting, organizing, distilling, sharing, developing and using information. One objective of the DoD Information Management & Information Technology Strategic Plan is using information as a strategic asset. Critical to this objective is the application of the theory of knowledge management. The importance of knowledge management is highlighted by indicating a knowledge management system within the DoD does not currently exist.[13]

In addition to inter-department information sharing gaps the DoD recognizes through this strategic plan, sharing information among coalition partners is a critical component. The DoD recognizes this importance and indicates its taking an active role in establishing an effective information sharing environment.[14] The more useful approach would be a detailed description of this environment but none truly exists within the latest published information management strategy.

Information Sharing Guidance and Strategy

Since the attacks of September 11, 2001 the ability to share information has been a hot topic at the most senior levels of our government. Attempts to provide guidance and directives aimed at sharing information internally, among executive departments, between government agencies and private sector partners, with foreign allied governments, and coalition partners. These attempts have consisted of executive orders signed by the President of the United States, departmental instructions, and strategic plans. These documents focus on strategic level and only touch on the capabilities at the operational and tactical levels.

Following the terrorist attacks on the United States in September 2001 information sharing inefficiencies were highlighted at the highest levels of our government. In response to these inefficiencies President Bush signed an executive order, Executive Order 13388, directing the sharing of intelligence information of potential terrorist threats among governmental agencies. Although 13388 does not discuss information sharing among coalition partners, it does identify the importance of having programs in place to share information simply by virtue of the level at which it was produced. The fact that the President recognized the importance of sharing information should serve as an indicator of the importance of this initiative within every facet of our government.

In February 2004 the Department of Defense authored a document to establish a standard for information sharing. This document was the DoD Instruction Number 8110.1 and would establish a technical tool known as Combined Enterprise Regional Information Exchange System (CENTRIXS) as the technical standard for multinational information sharing among coalition partners. This program was established initially in 1999 within U.S. Central Command. Following the attacks on the United States in September 2001 the program was accelerated.[15] In addition to this standard, this instruction "assigns responsibilities and provides procedures to standardize the means for connecting the DoD Components electronically to foreign nations on an Enterprise basis, and for allowing the secure, mutual exchange of operational and intelligence information in support of combined planning, a unity of effort, and decision superiority in multinational military operations."[16] Thirdly, this instruction "provides the guidance, framework, key principles, and interoperability processes for multinational information sharing networks, computing, information interoperability, that are part of the GIG [Global Information Grid]."[17]

CENTRIXS would later become one of the most commonly used technical means in Iraq and Afghanistan.

In May 2007 the Department of Defense Chief Information Officer, in response to the Quadrennial Defense Review (QDR), created an information sharing strategy.[18] This strategy develops an action oriented plan to achieve improved unity of effort, improved quality and speed of decision making, increased adaptability of forces, improved situational awareness, and greater precision in mission planning and execution. This strategy encompasses all governmental organizations, coalition partners, and unanticipated partners and establishes the Departmental foundation for strategic implementation planning.[19] It is recognized through this strategy that "effective information sharing enables the DoD to achieve dynamic situational awareness and enhance decision making to promote unity of effort across the Department and with external partners." The vision of this strategy is to "deliver the power of information to ensure mission success through an agile enterprise with freedom of maneuverability across the information environment."[20] This strategy is being implemented with four goals to achieve:

1. Promote, encourage, and incentivize sharing.
2. Achieve an extended enterprise.
3. Strengthen agility, in order to accommodate unanticipated partners and events.
4. Ensure trust across organizations.[21]

In order to meet these goals, an information sharing senior steering group has been established. This group will provide guidance and oversight of the program and synchronize the individual efforts to establish information sharing environments in order to create unity of effort.[22]

In addition to the information sharing strategy the Department of Defense developed the Information Management & Information Technology (IM/IT) Strategic Plan covering 2008 to 2009. The intent for this plan is to "provide a common understanding of a shared vision, mission and governing principles for IM/IT. The plan identifies specific goals and objectives to guide the net-centric transformation of the DoD. It will also define key performance indicators for assessing progress toward meeting the goals and objectives that will move the Department's transformation to net-centric information sharing from concept to reality."[23]

All of these documents highlight the importance of sharing information and provide a foundation for implementing plans to create an environment of information sharing. They set goals and objectives, metrics to measure performance, as well as implementation status, and are focused on many different aspects of information sharing. In addition to the technological challenges involved with sharing information, cultural, policy, and governance play an important role in sharing information.

Information sharing is complicated when coalition partners are included in military operations. The culture of the U.S. military is one of over-classifying information. This is due to potential risk of divulging information to the wrong organization. USCENTCOM leadership recognized this culture as a significant road-block to including coalition partners in operations.[24] The CENTCOM J6, Brigadier General Susan Lawrence, in a white paper on the topic of coalition information sharing in 2006 said a cultural shift would be required to resolve the problem of over classification.[25] This culture not only exists within USCENTCOM but within the DoD.[26] During a multinational operations conference in May 2008 the problem of over-classification was also

discussed. Bill Barlow, deputy director of the Integrated Information Communications Technology office within the OASD/NII stated "unclassified information sharing and collaboration with non-DoD entities continues to be problematic. The DoD culture is classify by default rather than share by default. Over-classification of documents, cumbersome policies, and ad hoc networks have led to distrust by non-government organizations (NGOs) and numerous civilian agencies."[27] The culture of over-classification has not been addressed in published guidance and will not be resolved until senior government leaders place true emphasis on the problem. Until guidance is published military leaders will continue to develop unique solutions to share information.

ANALYZING THE PROBLEM

A Commander's Perspective (The Tip of the Spear)

Lieutenant Colonel (promotable) Eric Welsh, currently serving as Special Assistant to the Chief of Staff of the Army, is an infantry officer and former Battalion Commander of 2nd Battalion, 7th Cavalry Regiment within the 4th Brigade Combat Team, 1st Cavalry Division. His unit was responsible for combat operations of the entire city of Mosul located in Northern Iraq from November 2006 to January 2007. LTC Welsh maintains a unique view of information sharing and relates his experience in Mosul as testament to his ideas. It is LTC Welsh's belief that communication is key to everything we do. From our everyday lives at home, with family and friends, to executing combat missions in Iraq, communications plays a significant role in all that we do. The ability to articulate ideas or directives in a clear and concise manner can lead to success if executed well. It can also lead to mission failure if not executed well. There are several

unique challenges that leaders like LTC Welsh dealt with in Iraq. From relationships to technical capability, to dealing with misinformation, there are many aspects of information sharing that impact decision making of our military commanders.

In a counterinsurgency conflict like Iraq, an approach very different from conventional operations is used to gather, analyze, and disseminate information. Gaining access to the public through relationships with civilian government leaders is critical. Developing a trust between military leaders and government officials can lead to key intelligence that results in the capture of high value insurgents. From a very different stand point it can help protect Soldiers conducting patrols. When the military leader prosecuting insurgency operations gains the trust and confidence of the local officials he is able to gain valuable information. LTC Welsh states "it's all about understanding culture and using that understanding to develop strong, trusting relationships."[28] He indicated his strong relationships with the local leadership within the police department as well as the city officials allowed his unit to capture or kill very senior leadership within the Al Qaeda organization in Mosul. He also indicated he believed these strong relationships built on mutual trust protected his soldiers. He also believed relationships were not as strong among military commanders and local civilian leaders following the departure of LTC Welsh's unit in early 2007. When discussing information sharing technical capabilities usually dominate the discussion. The technical capability was certainly not the most influential aspect of information sharing LTC Welsh relied on, it was personal relationships based on mutual trust and his understanding of the cultural differences that made the difference.

LTC Welsh's unit was, at the time, part of the newest brigade combat team the United States Army fielded. His unit maintained some of the most highly technical tools to support the execution of battle command. These tools were instrumental in providing situational awareness; however, LTC Welsh's ability to execute battle command, react to intelligence, and communicate was not tied to any particular technology. Communication within his unit was very horizontal, providing quick dissemination between patrols, subordinate commanders, staff, and himself. If intelligence was gained regarding potential targets LTC Welsh used a system of redundancy to confirm, before acting on the intelligence. Typically this confirmation was accomplished by using other technical means. This, he says, is how the technical aspects of his unit facilitated quick action on targets. LTC Welsh had a full array of technical communications and intelligence, surveillance, and reconnaissance systems to work with. From Blue Force Tracker in tactical ground vehicles to unmanned aerial vehicles, 2-7 Cav maintained the very latest in technology focused on information dominance. With all this technology available the single most reliable and under exploited tool LTC Welsh used to confirm intelligence before sending his Soldiers into potential hostile areas was the helicopter pilot armed with his eyes and a radio talking back to the 2-7 tactical operations center (TOC). It is this human aspect LTC Welsh relied on the most.[29]

2-7 Cav partnered with the Iraqi Security Forces (ISF) in all combat operations. Maintaining a good communications link with the ISF during operations proved difficult at times due to the lack of similar equipment. LTC Welsh's unit used a secure FM radio that hopped a frequency approximately 100 times per second to pass critical information within the unit that was secure. The ISF did not have a similar means of communication so all communication with them was unsecure and vulnerable to the enemy listening. This was a challenge that LTC Welsh was

not able to overcome. In some cases he knew the ISF unit he partnered with was infiltrated and possibly listening to these unsecure communications. Once this was understood it could be used as an advantage. He stated misinformation is sometimes just as helpful as intelligence. By disseminating misinformation, the ISF leadership would be able to determine who the infiltrator was and take steps to eliminate them from their ranks.

LTC Welsh and the soldiers of 2nd Battalion, 7th Cavalry Regiment met significant successes during their 15 month deployment to Iraq. The battalion was able to capture or kill numerous senior level Al Quieda leaders, assist the ISF with the development of a capable security force, and save thousands of Iraqi lives by reducing hundreds of improvised explosive devices (IEDs). All of the operations focused on these three goals were not possible without information sharing, but, not through email, SIPRNET, NIPRNET, UAVs, and other technical tools. Their success was due to good relationships with local leaders built on mutual respect, trust and an understanding of each other's culture. Sometimes the best ways to share information do not cost a thing, they just require leaders to recognize the complexities of their environment and understand the differences in culture.

A Commanders Perspective (Supporting the Fight)

To gain a different perspective on information sharing capabilities, requirements, and challenges one should ask the person responsible for installing, operating, and maintaining the systems used to facilitate it. The capabilities, requirements, and challenges are certainly different for the commander charged with supporting the fight. One such officer is Colonel Joseph Layton. COL Layton is a U.S. Army signal officer who has served in key staff positions and commanded

soldiers supporting the communications infrastructure providing the capability to share information among the entire coalition in Iraq. In an interview with COL Layton, he discussed some of the collaborative tools used to plan and track operations, the introduction of non-standard equipment to expand the infrastructure and the difficulty supporting this equipment.

The First Cavalry Division entered Iraq in 2004 for a yearlong rotation. During their first rotation COL Layton served as the First Cavalry Division G6, responsible for coordinating all communications systems used for command and control of the division. During this rotation there were three technological advances in communications and information sharing capability that really enhanced commander's ability to collaborate, execute battle command, and share information among the coalition. The installation of a voice network relayed along many common routes through Iraq now known as RIPRnet (Radio Internet Protocol Routed Network), the standardization of collaborative planning and operational tools, and the distribution of CENTRIXS to communicate with coalition partners. These three advances have become the Army standard for each of the functions they serve and are common in all units rotating into Iraq.[30]

The common radio used for mobile command and control of every U.S. ground unit in the Iraqi operational area is the FM radio. This radio is not effective beyond approximately 30 kilometers. Due to the long convoy routes and large operational areas this range was not enough. The idea to install a relay network along the most commonly traveled routes and in key locations in each operational area would extend the range of these radios. This radio relay network would also facilitate communications for coalition partners because one frequency was left unsecure. The common name for the non-secure frequency is the sheriffs net. Any units that find themselves in

contact or stranded along a route can tune to this non-secure frequency and contact someone for assistance. This relay network has expanded and is now relayed through a series of commercial radios and computer systems creating a robust and reliable network known as the RIPRnet that is available to the entire coalition.[31]

During the initial few months in theater several tools were in use for internal collaboration. Commanders needed a single tool that would allow real time collaboration, display the common operational picture, and can be used for planning. The problem commanders were running into was to conduct each of these activities a different tool had to be used. These individual tools provided the functionality for a particular task but could not talk to each other. The decision was made by the Division Commander to introduce the Command Post of the Future (CPOF). This tool allowed commanders to talk to each other, use a white board tool, display and manipulate graphics, plan, track operations, and serve as the common operational picture.[32] From early 2004, CPOF has evolved into the Army standard for the entire theater. The problem with CPOF is the U.S. only classification. Because of its classification, it can only be used by U.S. forces leaving coalition partners out of the information loop.

In order to bring coalition partners into the information sharing environment CENTRIXS was used as the standard information system. This system is composed of utilities such as email, web based applications, and data sharing servers, similar to systems already in use on U.S. only networks. These utilities are placed on infrastructure that is separate from the U.S. only networks either physically or virtually using tunneling technology. Tunneling is a technology that virtually separates networks using a single infrastructure. This separation allows non-U.S. forces the

capability to use these systems for the purpose of information sharing, enhanced situational awareness of the coalition, and more efficient operational planning.[33] CENTRIXS has been an integral part of developing the link between U.S. and other coalition forces and has realized significant expansion since its initial establishment during the early part of Operation Iraqi Freedom.

As a battalion commander of a signal unit, COL Layton dealt with a different set of challenges that impacted communications and information sharing capabilities than the infantryman. COL Layton's unit was responsible for installing the U.S. Army's standard communications equipment. This equipment was called Mobile Subscriber Equipment (MSE), and was introduced to the Army in the early 1990's. Upon deployment to Iraq, for the second time, COL Layton discovered a significant change with respect to infrastructure. His mission would not consist of using his MSE systems but managing large technical control facilities consisting of commercial equipment. His Soldiers, trained to install specific aspects of MSE systems, would be required to learn these new systems while supporting units who were actively conducting combat operations. These new facilities, although complicated, provided a fixed infrastructure with much greater capacity to support the information sharing tools used by the coalition in Iraq. In addition to providing the infrastructure necessary for these information sharing tools, it allowed the distribution of these systems to lower echelons not typically considered supportable by typical standards. These information sharing tools were now available to the lowest tactical levels allowing the soldiers conducting patrols access to critical information. It is because of the ability to push these systems down to the lowest tactical level that the information sharing example outlined earlier was able to occur. COL Layton explained the successful expansion of

communications networks in Iraq was not a result of doctrinal changes or operational decisions made by the Signal Center at Fort Gordon. It was because of the hard work by dedicated signal soldiers learning these new facilities and ensuring the static infrastructure was run efficiently.[34]

The Iraqi Security Force as a Coalition Partner

Is the Iraqi Security Forces (ISF) a coalition partner of the United States in Iraq? At the tactical level in Iraq most of the coalition interaction occurs with the ISF. As the priority in Iraq shifts to transitioning the operational lead from U.S. Forces to the ISF, conducting joint operations with ISF units is more common. To facilitate this transition, Military Transition Teams (MiTT) have been embedded with regular ISF units at every level from battalion up. These MiTTs are generally small 12 to 15 man teams consisting of various specialties. One particular transition team lead by COL Mike Senters, advised an Iraqi army brigade in Mosul, Iraq from 2006 to 2007. In an interview, COL Senters discussed information sharing techniques, challenges, lost opportunities, and some ideas to improve unity of effort among U.S. Forces and the ISF.

Senters explained the ISF operating in Mosul, Iraq typically operate using commercial of the shelf automation equipment, cellular telephones, and radios to execute battle command. None of these devices are operated with encryption making communications vulnerable to enemy monitoring and potentially compromising future operations. Based on my experience in Iraq this is consistent with all communications systems in use by the ISF for command and control. Information sharing between the ISF and U.S. forces typically occurred using commercially provided internet systems and sometimes email accounts from providers such as Yahoo and Google.[35] When conducting joint operations with U.S. Forces, the transition team had the

capability to serve as the communications link between U.S. and ISF. Another option sometimes used by U.S. commanders in these joint operations was to operate a commercial radio on the same frequency as the ISF and accept the risk of being monitored and potentially compromised. Because of the immature state of the ISF, equipment for command and control was very basic. COL Senters explained the ideal situation would have been for the ISF to establish a closed local area network (LAN) within the brigade to facilitate a very basic digital capability used for information sharing. He also stated that although information sharing is important, it was not a priority during his rotation in Northern Iraq.[36]

The ISF incurred significantly more challenges than typical coalition partners such as the British or Australians. The capacity for the ISF to establish, manage, and expand a communications network was not available. COL Senters indicated the focus was much more basic such as recruiting soldiers, learning basic combat drills, and developing standards. These basic functions are typically taken for granted within mature military forces but must be developed in a military in its infancy such as the ISF. These basic functions took priority to developing a robust communications network.[37] Another challenge was the lack of operational security or training within the ISF to maintain this communications architecture. Unfortunately there are members of the ISF that are compassionate to the cause of some insurgent groups. This causes challenges with operational security and availability of a network within the ISF would facilitate these individuals' efforts to compromise operations. COL Senters acknowledges these groups exist within the ranks of the ISF; however, he is also adamant that many of the soldiers he advised were patriots and were focused on rebuilding Iraq and the ISF.[38]

Although many challenges exist within the ISF there are lost opportunities because of poor information sharing initiatives between the U.S. and ISF. The U.S. military has the capability to analyze electronic devices such as cellular telephones and computers captured from insurgent groups. The ISF routinely conducts raids of suspected insurgent locations and captures these devices. Because the U.S. is not aware of the captured devices intelligence is lost because these devices are not analyzed for information. In addition to electronic devices, basic documents such as captured identification cards are not turned over to the U.S. The U.S. has an initiative to collect and store biometric and other identification data of potential insurgents. Because the U.S. is not aware of the ISF capturing the documents the opportunity to expand this data is lost.[39] This is just a single example from a single brigade of lost opportunities due to gaps in information sharing. If these information gaps were closed it would surely aid in the defeat of the insurgency within Iraq.

One suggestion made to facilitate information sharing is a combined tactical operations center (TOC). COL Senters suggested if U.S. units combined TOCs with ISF units the information gaps could be closed. The information collected by both U.S. and ISF units would be shared and intelligence would not be lost as it is currently. Operational situational awareness would be enhanced and unity of effort would be achieved. This relationship would also serve to allow the ISF to be treated more like a coalition partner. This idea comes with challenges such as operational security but there are enough trusted soldiers within the ISF to make this idea work.[40]

There is no doubt the ISF has challenges. The expectation that a force such as this would not have challenges in its infancy is unrealistic. Information sharing challenges, developing basic soldier standards, and rooting out those who are compassionate toward the enemy are the common

challenges faced by the ISF. With all these challenges, leaders at the tactical level, within both the U.S. military and the ISF, continue to develop unique solutions to defeat the insurgency while developing a mature ISF. So, is the ISF a coalition partner? The ISF does not receive the same level of trust that conventional coalition partners receive; however, it is not inconceivable to believe the ISF could reach a level of competency to operate independently in the future.

CENTRIXS, the Only Way Ahead?

Communications networks supporting information sharing requirements of our military commanders are a permanent fixture in modern warfare. Not only the U.S. military but other military's have integrated these robust information systems into their tactics, techniques, and procedures. In our global environment, "we do nothing by ourselves...multinational operations are the norm today in combat, stability operations, or in crisis intervention."[41] Having a system to share information with these partners is critical. In the net-centric environment we now operate, to plan effectively, develop unity of effort, and exchange operational intelligence a common information system is required. As identified earlier the Combined Enterprise Regional Information Exchange System (CENTRIXS) has been identified as the standard. "CENTRIXS system allows the Coalition and its allies to securely exchange mission-specific operational and intelligence information with our coalition and mission partners."[42] "The DoD developed the CENTRIXS program to facilitate classified information exchange between the U.S. and coalition partners at the strategic down to the tactical levels."[43] This system, unfortunately, is the only major initiative developed to facilitate multi-national information sharing. In order to understand

CENTRIXS and I'll focus on some background information, its current capabilities, and the vision for CENTRIXS and information sharing in the future.

In the net-centric environment technology is the corner stone for information sharing. Many different aspects impact information sharing but the foundation in the new environment is technology. In early 1999, USCENTCOM began an initiative to develop a technical platform to share information with coalition partners. Realizing operations would not be unilateral and the importance for multinational information the initiative was started to develop CENTRIXS. Later that year "the Interoperability Senior Steering Group (ISSG) was formed as one of the Director, Defense Intelligence Agency's (DIA) four major thrust areas to focus the efforts of the defense intelligence community."[44] Following September 11, 2001 it was realized CENTCOM would begin operations in Afghanistan (Operation Enduring Freedom) and the capability for the coalition to have a common operational picture (COP), common intelligence picture (CIP), and information sharing was needed. Focus was applied to speeding the development of CENTRIXS to meet these requirements.[45] After operations began in Afghanistan and Iraq, the DoD provided an instruction (DoD Instruction Number 8110.1, Feb 04) to develop CENTRIXS as the standard for DoD information sharing. CENTRIXS is now the system used for information sharing among coalition partners.

The core functionality of CENTRIXS is email, web based data access, imagery, collaboration, and standard Microsoft Office tools. These functions operate on commercial off the shelf (COTS) computers and servers. These services are connected using current infrastructure but are virtually separated using tunneling technology. This technology allows a single network infrastructure to act as a separate environment keeping CENTRIXS separate from other systems.

Figure 1

Figure 2

Figures one and two show the COTS equipment used to support CENTRIXS. Clients are attached to the CENTRIXS network using typical COTS computer systems (figure 1). The server side (figure 2) consists of COTS computer servers that support email, web data access, and other services.[46] All of this data is encrypted using an encryption device and communications security key that is releasable to coalition forces using this system. CENTRIXS is virtually identical to many of the systems in use by the U.S. military. Because of this similarity users and administrators require very little training to use or support CENTRIXS.

CENTRIXS does not come without several challenges that have yet to be solved. Although the system traverses the same network infrastructure as other battle command systems it is still a separate system requiring a dedicated computer. Those that operate on multiple systems must maintain a computer for each system. For example, if a staff officer receives non-secure (NIPRNET), secret (SIPRNET), and CENTRIXS email three computers would be required. If the CENTRIXS and SIPRNET were collapsed into a single computer systems capable of operating on both networks USCENTCOM alone could save $212 million.[47] This separation is due to security policies and a culture that tends to over-classify information. In addition to CENTRIXS being

separated from other U.S. only networks each CENTRIXS network is kept isolated. For example, the CENTRIXS network supporting Iraq is separate from the CENTRIXS network supporting Afghanistan even though they are both within the USCENTCOM area of responsibility.[48] Again, an overly secretive culture has led to this separation which hinders information sharing within the USCENTCOM AOR. In addition to the challenges faced by separation an equal share of funding for information sharing technology does not exist. In many cases coalition partners lack the financial capacity to fund initiatives for information sharing. An example is the budget allocation for information technology within the Afghan security forces in 2006 was only $25,000 for a complete year.[49] This small amount allocated for technology precludes this force from investing in technology such as CENTRIXS. In an environment where the United States operates with nations in this situation the question of funding becomes a limiting factor. It is no secret that information sharing is imperative but should the United States and other western nations be responsible for funding systems of underdeveloped nations?[50] This also inhibits the sharing of information among coalitions. Technology is available to resolve some of these conflicts, it would simply take a change in culture; however, the question of financing will most likely require tough decisions by leaders at the most senior levels of our government.

CONCLUSIONS & RECOMMENDATIONS

In a relatively short amount of time, the Gulf War of the early 90's to current operations in OIF and OEF, the United States military has recognized the benefits of a network centric force. The technological revolution has provided commanders an information advantage never before realized in modern warfare. The ability to connect the tactical level of war to the most strategic levels of the United States government has been captivating. This capability has also caused great

debate focused on leveraging this new way of information sharing. From presidential guidance, to Department of Defense directives and the creation of working groups made up of senior leaders, there have been many initiatives to guide solutions for information sharing internally, cross-department, as well as with foreign mission partners; however, before the benefits of information sharing are truly realized a change in culture will be required.

As shown at the tactical level through the example of LTC Welsh's 2-7 Cav, technology does not necessarily equate to successful information sharing. The tactical commander is not completely tied to any type of technology and relies on relationships built on mutual trust. These relationships facilitated successful information sharing between Iraqi's in LTC Welsh's battle space enabling his unit to gather useful intelligence and take action. These relationships were developed through an understanding of each culture and leaders recognizing the importance of having a face-to-face dialog that resulted in successful sharing of information. This is not to say technology does not play a role. Technology can enhance the commander's ability to execute battle command; however, it does not tie the hands of tactical commanders.

As attention is moved to the operational and strategic levels, technology plays a much more significant role in successful information sharing. It is at these levels that tools such as CENTRIXS is available and crucial for sharing information among coalition partners. The CENTRIXS system is very similar to many battle command systems already in use but is separated from U.S. only information systems. This separation is put in place to ensure information not releasable to other countries, is not inadvertently transmitted to an unauthorized source. This separation causes gaps in information sharing capability resulting in inefficient processes and

strain on resources. Although guidance from the most senior levels directs the sharing of information, a culture of over-classifying information and a varying degree of interpretations of information sharing policies has kept some technological solutions separated. A different fiscal position among coalition partners has caused many to question the reality of developing a true synergy from information sharing technologies.

Information sharing among coalition partners is taking place, although, it could be much more efficient if some of the barriers were taken down. Tactical commanders rely on face to face meetings for coalition information sharing. Operational commanders have the technology in place to facilitate information sharing but lack efficiency due to cultural and fiscal challenges. Strategic level guidance is general and fails to provide a detailed road map for the successful implementation for leveraging technology to share information. Even with these challenges, units currently engaged in combat operations are developing unique solutions to achieve unity of effort in a coalition environment. A cultural shift regarding restrictive policies will be required to achieve the benefits of information sharing. Once these policies are in place technological advancements will be required to merge current information systems using guards to filter information ensuring only authorized data is passed to coalition partners. This technology is available and could very easily be implemented; however, it will not be reality until policies are changed and a common understanding of already published guidance exists.

End Notes

[1] Boland, "CENTCOM Pursues Assured, Interoperable Communications", 1.
[2] Herring, "Network-Centric Warefare – Effective or Information Overload," April 2006, 2.
[3] DoD Information Sharing Strategy, May 2007.
[4] IBID.
[5] IBID.
[6] IBID.
[7] IBID.
[8] Twitty, Interview, Jan 09.
[9] IBID.
[10] IBID.
[11] Stewart, Interview, Jan 09.
[12] DoD Information Management & Information Technology Strategic Plan, 9.
[13] IBID, 6.
[14] IBID, 7.
[15] Boardman, ISSG, 5.
[16] DoD Instruction 8110.1, Feb 06, 1.
[17] IBID, 2.
[18] DoD Information Sharing Strategy, May 2007, 1.
[19] IBID, 2.
[20] IBID, 3.
[21] IBID, 3.
[22] IBID, 1.
[23] IM/IT Strategic Plan, I.
[24] D'Ippolita, "Coalition Information Sharing", Apr 07, 18.
[25] IBID.
[26] IBID.
[27] McDade, "Information Sharing Challenges on a Multinational Scale," Sep 08, 4.
[28] Welsh, Interview, Jan 09.
[29] IBID.
[30] Layton, Interview, Jan 09.
[31] IBID.
[32] IBID.
[33] IBID.
[34] IBID.
[35] Miller, Interview, Dec 08.
[36] Senters, Interview, Jan 09.
[37] IBID.
[38] IBID.

[39] IBID.
[40] IBID.
[41] McDade, "Information Sharing Challenges on a Multinational Scale," Sep 08, 1.
[42] EDS CENTRIXS Fact Sheet, Jun 07, 1.
[43] D'Ippolito, "Coalition Information Sharing," Apr 07, 13.
[44] Boardman, ISSG, 5.
[45] IBID, 6.
[46] EDS CENTRIXS Fact Sheet, Jun 07, 1.
[47] McDade, Evy, "Information Sharing Challenges on a Multinational Scale." Sep 08, 3.
[48] Boardman, CENTRIXS, Supporting Coalition Warfare Worldwide. 11.
[49] Boland, Rita, "CENTCOM Pursues Assured, Interoperable Communications", 4.
[50] IBID.

Bibliography

Ackerman, Robert K. "Data Holds the Key to Network-Centricity." *SIGNAL Magazine* (2005), http://www.afcea.org/signal/articles/anmviewer.asp?a=613&print=yes.

———. "In NATO, Technology Challenges Yield to Political Interoperability Hurdles." *SIGNAL Magazine* (2006), http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=1088&zoneid=176.

"African Nations Prepare to Test Communications Systems " *American Forces Press Service* (2006), http://72.14.209.104/search?q=cache:DLaagHc6jnQJ:www.defenselink.mil/news/Feb2006/20060217_4233.html+africa+endeavor+communications&hl=en&ct=clnk&cd=1&gl=us.

ASD(NII)/DoD_CIO. "Department of Defense Instruction Number 8110.1 Multinational Information Sharing Networks Implementation." Department of Defense, 2004.

Boardman, Jill. "Interoperability Senior Steering Group Efforts to Build a Global Data Network for Joint Coalition Warfighting." 11. Macdill AFB: USCENTCOM, 200X.

Boardman, Jill L. "Combined Enterprise Regional Information Exchange System (CENTRIXS); Supporting Coalition Warfare World-Wide." 15. MacDill AFB, FL: CENTCOM, 2004.

Boland, Rita. "CENTCOM Pursues Assured, Interoperable Communications." *SIGNAL Magazine* (2006), http://www.afcea.org/signal/articles/anmviewr.asp?a=1203&print=yes.

———. "Network Centricity Requires More than Circuits and Wires," Armed Forces Communications and Electronics Association, http://www.afcea.org, September 2006.

Dale, Helle. "NATO in Afghanistan: A Test Case for Future Missions (Draft)." *The Heritage Foundation* (2006), http://www.heritage.org/Research/MiddleEast/bg1985.cfm.

D'Ippolito, Andrew S., Major, U.S. Air Force, "Coalition Information Sharing: The Global War on Terrorism Requires Global Partnerships." April 2007.

Electronic Data Systems (EDS) Fact Sheet, Combined Enterprise Regional Information Exchange System Overview (CENTRIXS), June 2007.

Herring, Terry W. "Network-Centric Warefare – Effective or Information Overload," April 2006, Air Command and Staff College, Maxwell AFB, AL.

"Information Management and Information Technology Strategic Plan 2008 – 2009," Washington D.C. 2008

"Information Sharing Strategy," Washington D.C.: Department of Defense, May 2007

Layton, Joseph COL., Former Division G6 and Signal Battalion Commander, Interview, 30 January 2009.

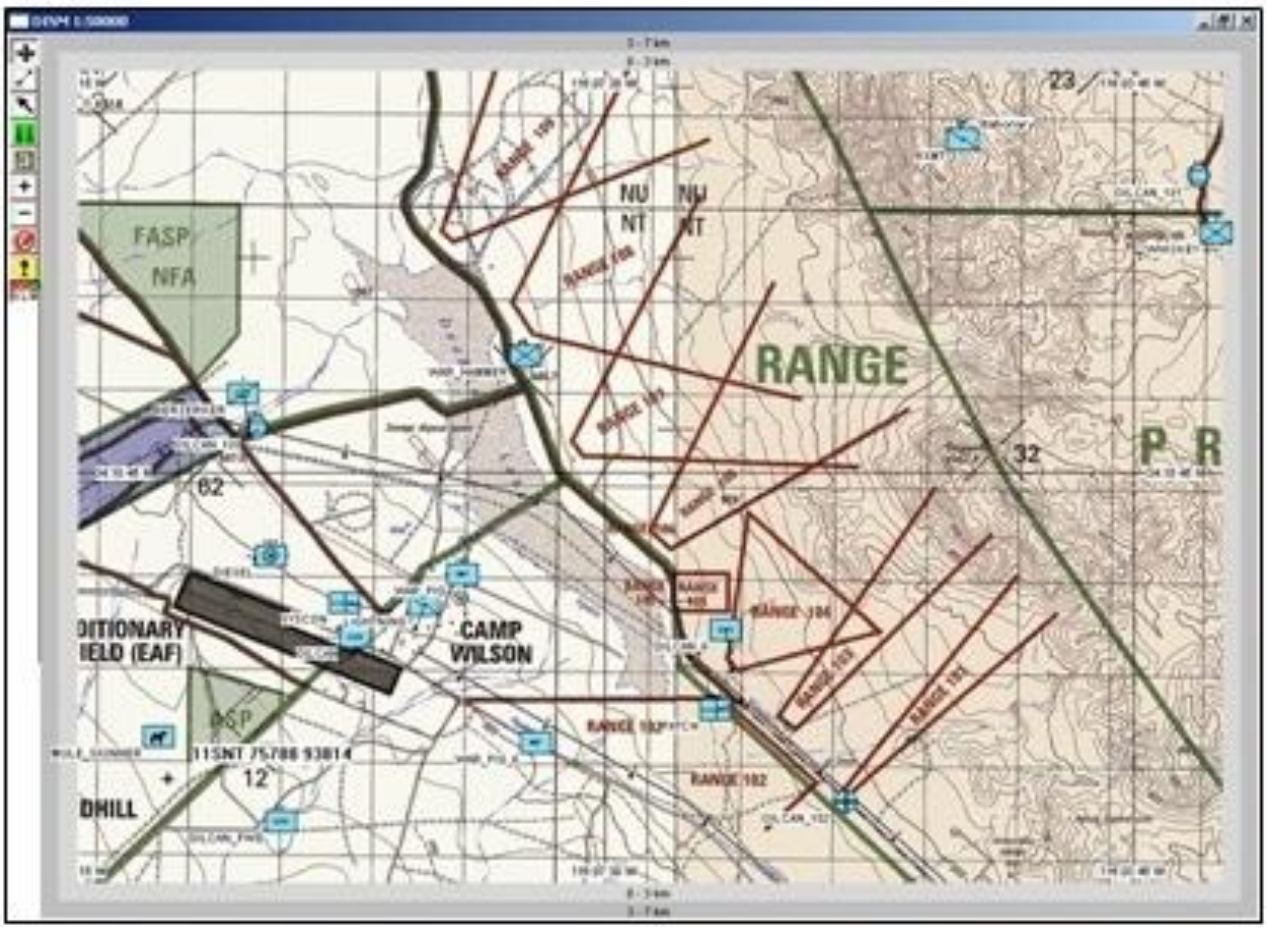
McDade, Evy. "Information Sharing Challenges on a Multinational Scale," http://www.mitre.org/news/digest/defense_intelligence/09_08/multiops.html, September 2008.

Mawby, David, Ian McDougall, and Greg Boehmer (PA US). "A Network-Centric Operations Case Study: US/UK Coalition Combat Operations During Operation Iraqi Freedom." edited by Office of Force Transformation, 136, 2005.

Miller, Matthew Captain. Former Signal Officer, 1st Battalion, 9th Cavalry Regiment and Transition Team Support, Interview, December 2008.

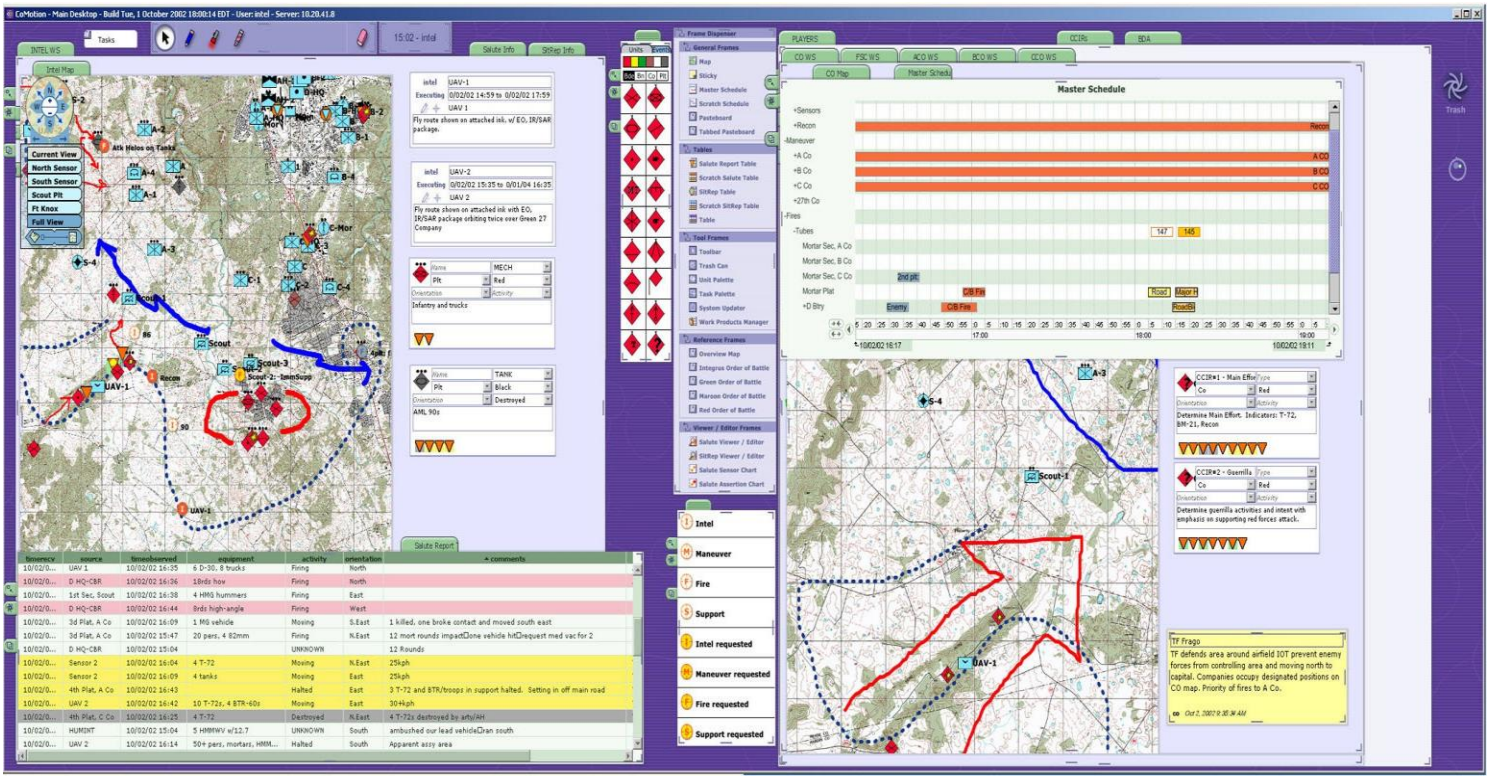
"National Strategy for Information Sharing," Washington D.C. October 2007
Parker, RL. "A NATO Perspective on CENTRIXS." no. DRAFT ver. 0.9 (2005), http://www.dodccrp.org/events/10th_ICCRTS/CD/papers/007.pdf.
Parker, RL. "A NATO Perspective on CENTRIXS Presentation," http://www.dodccrp.org/events/10th_ICCRTS/CD/presentation/007.pdf.
Schmith, Michelle D. "Do We Make Interoperability a High Enough Priority Today?" Air University, 2001.
Stewart, Jeff, LTC, Former BCT Operations Officer, 4th BCT, 1st Cavalry Division, Telephonic Interview, January 20, 2009.
Stewart, Keith G. "11th ICCRTS Coalition Command and Control in the Networked Era: Mission Command in the Networked Era." http://www.dodccrp.org/events/11thICCRTS/html/papers/026.pdf, June 2006
"Technologies Empower Coalition Information Sharing; but Not All Interoperability Challenges Are Equipment Based." *Digital Signal Magazine* (2006), http://www.afcea.org/signal/articles/anmviewer.asp?a=1175&print=yes.
Twitty, Stephen COL, Former BCT Commander, 4th BCT, 1st Cavalry Division, Telephonic interview, January 27, 2009.
Welsh, Eric LTC (p), Former Battalion Commander, 2d Battalion 7th Cavalry Regiment, Telephonic interview, January 23, 2009.

Appendix A – Blue Force Tracker



Blue Force Tracker is a situational awareness tool that incorporates mapping software and provides leaders with friendly and enemy locations, graphical references, and a messaging capability similar to email. It's intuitive graphical user interface ensures users can quickly manipulate the various functions using either a keyboard or a touch screen. This tool has revolutionized information sharing among U.S. military organizations and continues to receive enhancements focused on providing real time information from the tactical to operational levels of war.

Appendix B – Command Post of the Future



This picture is an example of the graphical common operational picture provided by Command Post of the Future. On a single computer, operations officers are able to track friendly forces, enemy forces, significant activities, timelines, as well as collaborate with others within the environment in real time. This common operational picture receives data from other battle command systems (ASAS, AFATDS, BFT, BCS3) creating a true common operational picture.