Strategy Research Project

COALITION MISSION COMMAND: BALANCING INFORMATION SECURITY AND SHARING REQUIREMENTS

BY

COLONEL JONAS VOGELHUT
United States Army

USAWC CLASS OF 2011

U.S. Army War College, Carlisle Barracks, PA 17013-5050

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
28-02-2011	Strategy Research Project	

4. TITLE AND SUBTITLE

Coalition Mission Command: Balancing Information Security and Sharing Requirements

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Colonel Jonas Vogelhut

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Dr. Jeffrey L. Groh
Department of Distance Education

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution A: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

As the United States expands its use of coalitions in future combat operations, commanders will face challenges of when and how much information to share to be effective versus security concerns. U.S. military forces must develop and implement policies, processes, and technology to share sensitive mission command information with coalition partners, finding the balance between sufficient disclosures to enhance combat operations with protection against unauthorized release of information which would jeopardize combat operations. Current policy and international agreements form the basis for information sharing, but such strategic documents are insufficient to assist commanders guide subordinate leaders in fast moving tactical combat situations. This paper reviews the background of coalition information sharing, discussing the Afghan Mission Network (AMN) currently used in Afghanistan. Using a U.S. Intelligence Community model to assess information sharing, this document examines the AMN in five critical areas, assessing future risk and presenting recommendations to assist future policymakers support commanders faced with balancing information sharing with information security requirements.

15. SUBJECT TERMS

Network Centric Warfare, Afghan Mission Network, Cyber, Data

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	32	

USAWC STRATEGY RESEARCH PROJECT

COALITION MISSION COMMAND: BALANCING INFORMATION SECURITY AND SHARING REQUIREMENTS

by

Colonel Jonas Vogelhut
United States Army

Dr. Jeffrey L. Groh
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Colonel Jonas Vogelhut

TITLE: Coalition Mission Command: Balancing Information Security and Sharing Requirements

FORMAT: Strategy Research Project

DATE: 28 February 2011 WORD COUNT: 5,868 PAGES: 32

KEY TERMS: Network Centric Warfare, Afghan Mission Network, Cyber, Data

CLASSIFICATION: Unclassified

As the United States expands its use of coalitions in future combat operations, commanders will face challenges of when and how much information to share to be effective versus security concerns. U.S. military forces must develop and implement policies, processes, and technology to share sensitive mission command information with coalition partners, finding the balance between sufficient disclosures to enhance combat operations with protection against unauthorized release of information which would jeopardize combat operations. Current policy and international agreements form the basis for information sharing, but such strategic documents are insufficient to assist commanders guide subordinate leaders in fast moving tactical combat situations. This paper reviews the background of coalition information sharing, discussing the Afghan Mission Network (AMN) currently used in Afghanistan. Using a U.S. Intelligence Community model to assess information sharing, this document examines the AMN in five critical areas, assessing future risk and presenting recommendations to assist future policymakers support commanders faced with balancing information sharing with information security requirements.

COALITION MISSION COMMAND: BALANCING INFORMATION SECURITY AND SHARING REQUIREMENTS

The 2010 United States National Security Strategy states that “the foundation of United States, regional, and global security will remain America’s relations with our allies, and our commitment to their security is unshakable.”[1] The 2008 National Defense Strategy reinforces this imperative by stating victory against violent extremist groups and other threats require the United States to “apply all elements of national power in partnership with old allies and new partners”[2] and that “the long war is ultimately not winnable without them.”[3] As the future of military operations expands the use of coalitions rather than single nation efforts, commanders will continue to face the challenge of when and how much information to share to be effective. Idealistically, sharing all information with coalition partners would enhance overall situational awareness and improve decision making by creating a common operational picture, yet the same information may also be used against friendly operations, such as by revealing friendly locations vulnerable to attack, thereby weakening mission effectiveness.

Historically, coalitions primarily shared information through active delivery of information. Liaison officers, either stationed at or constantly visiting battlefield operations centers, would attend meetings and receive operations orders, limiting the information to those specific sheets of paper, briefing slides, or notes taken. With the use of distributed computers, networks, and data repositories, commanders today passively share more information with larger audiences. Organizations share this information with increased expectations on speed (time to get the information), users

(who can get the information), and scope (how much information users receive.) Looking at the current use of coalition forces in Afghanistan, the distribution of forces has dynamically changed from previous conflicts such as Operation Desert Storm or World War II. United States and Coalition partners routinely collate, intermingle, or task organize their militaries to meet battlefield requirements, necessitating the increased sharing of relevant mission command information such as force allocation, force protection, supply routes, and tracking movement of enemy forces. To meet this need within Afghanistan for Operation Enduring Freedom, the North Atlantic Treaty Organization (NATO), along with the United States, developed the Afghan Mission Network (AMN), specifically to "foster collaboration and information sharing by all International Security Assistance Force (ISAF) Troop Contributing Nations (TCN)."[4] For the future, the sharing of information across the coalition mission command systems, such as the AMN, must overcome challenges in sharing with coalition partners, finding the balance between sufficient disclosures to enhance combat operations with protection against unauthorized release of information which would jeopardize U. S. combat operations. To overcome these challenges the United States military forces must develop, improve, and implement policies, processes, and technology to share rapidly and effectively sensitive mission command information with coalition partners.

This paper begins with a review of the background of coalition information sharing, and introduces the benefits for both the United States and other nations. Next, several ongoing efforts in information sharing are discussed, including the AMN currently used in Afghanistan. Using a United States Intelligence Communities model to assess information sharing, this document reviews the use of the AMN in five critical

areas, providing potential explanations and assessment of future risk. Relying on these explanations, this author presents five recommendations to assist future policymakers to support commanders faced with balancing information sharing with information security requirements.

The Need for Information Sharing

Since the role of the U.S. military is to win the nation's wars, promote national security and protect national interests, military forces must prepare and train for combat operations. Any large-scale participation of United States forces will likely begin with coalition partners, such as participants from NATO, and commanders "will be required to share intelligence with foreign military forces and to coordinate receiving intelligence from those forces."[5] At the national level of government, the United States has published numerous forms of guidance emphasizing the need to share information with coalition partners. The National Strategic Plan for the War on Terrorism (4 March 2005) states the idea "…it is important that the United States have the capability to form multinational coalitions … [since] coalitions can contribute significantly to mission accomplishment."[6] The National Strategy for Information Sharing (NSIS) (October 2007) includes guidance stating that "The exchange of information should be the rule, not the exception, in our efforts to combat the terrorist threat."[7] This strategy (NSIS) provides the assessment that the United States should work harder to improve information sharing with foreign governments.[8] In balance with the idea of sharing with coalition partners is the need to share only appropriate information "with foreign governments to ensure appropriate security and confidentiality of exchanged information."[9] The Congressional Research Service advised Congress to add Networking with Coalition Partners to its list of oversight issues to improve the understanding of benefits and risks

associated with coalition information sharing.[10] The United States Intelligence Community (US IC) published its Information Sharing Strategy in February 2008 calling out the need to manage the risk between information protection and the challenge of missing clues to enemy attacks, costing lives and potentially endangering the national security of the United States.[11] This document lays out a five point model for the key questions to ask when considering information sharing, to include the need for information management (governance), the need for rules for sharing (policy), technology to enable sharing and security, establishing a culture of sharing, and finally obtaining the resources to share effectively the information.[12] Adapting this model to the issue of rapidly sharing mission command information within the current coalition of forces in Afghanistan and future coalitions, this document provides recommendations to improve future operations.

In 1597, Sir Francis Bacon proclaimed that “knowledge is power.” Leaders having as complete as possible understanding of a situation enhances mission effectiveness and reduces risk of negative consequences to their organizations. This quote works for both forces inside a coalition and adversaries looking to defeat the coalition. If an enemy force can gain vital information on troop locations, equipment capabilities and readiness, or unguarded avenues of advance, adversaries can use this information against coalition forces and change potential overmatch in capability to defeat or stalemate. One example is the potential damage from the Wikileaks disclosure of United States classified tactical military operations in Iraq and Afghanistan. Secretary of Defense Robert Gates stated that the release of the names of cooperative Afghan nationals in these documents are “…likely to cause significant harm or damage

to the national security interests of the United States…"[13] This damage could come from the murder of these supportive Afghan nationals by unsupportive Al Qaeda operatives or the destruction of the towns where these nationals live, where each negative act could degrade ongoing nation building activities in the region.

Within coalitions, the United States shares multiple forms of information with other nations and contributing partners, each with varied levels of nation-to-nation partnering experience and trust. Sharing of information becomes more complex as you share outside of your own organization to other government agencies[14], and then to coalition partners. Coalition information sharing begins with communications of administrative matters such as routine electronic mail, which becomes slightly more complicated with inclusion of attachments of the sharing of classified mail. Sharing continues up levels of complexity through common access to information (such as databases, file systems, etc.), to current mission command information (such as common operational and logistics pictures, unmanned aerial vehicles videos, and ongoing battlefield operations (artillery missions, aviation strikes, etc.)). Commanders must be aware of the limits of sharing information with coalition partners,[15] and should make informed decisions as to when and what level of information to share with each coalition partner, relying on foreign disclosure officers and international agreements[16] for each nation. Also involved in this balancing act is the assessment of the operational risk of sharing a different amount of information with participating nations, potentially disrupting atmospheres of trust and camaraderie, leading to diplomatic issues.[17] Operational risks that are too high in either probability of occurrence or consequence (or

both) can degrade the ability of an organization to execute strategy successfully within acceptable impacts to operations.[18]

For the current conflict in Afghanistan, the AMN integrates approximately 45 different nations into a secure information sharing environment to meet the mission command needs of regional military forces. During the year-long process to create this network, the United States Central Command (CENTCOM) shifted information that was only previously available through the United States classified network to the coalition network, including critical applications handling warfighter mission areas such as operational environment management, joint fires, joint intelligence and area force protection.[19] For each of these 45 nations, a separate international agreement[20] (or alliance[21]) is in place to identify what information leaders can share and remain in compliance with Executive Order 13526, Classified National Security Information (January 2010). Within the United States Pacific Command, the command coordinates with up to 39 nations, managing several programs supporting coalition operations, (such as the Combined Communications Interoperability Program) based on individual regional partner security agreements.[22]

Challenges arise when local commanders face new situations, under time constraints such as changes in unit locations which require new task organizations and partnership. For example, when the United States co-occupies a forward operating base with other nations, other nations may request insight to unmanned aerial video system information or pictures from Persistent Threat Detection System cameras. Although these systems can provide valuable information on enemy troop movements, some international agreements may not include updated access to these capabilities. A

recent example of this issue emerged in South Kandahar, Afghanistan, where 18 nations, including forces from the United States, United Kingdom, Canada and Australia could not see or talk to each other since they were on different secure networks.[23] Other challenges may arise when the co-located troop contributing nation does not have technologically equivalent equipment required for the information sharing and asks local commanders for use of equipment to ensure a common understanding of the battlefield.[24] Coalition forces must develop both the capability and willingness to securely share and coordinate across organizations to maximize effectiveness in combat.

The Need to Securely Share

As leaders continue to form, modify, disestablish and recreate coalitions to meet mission requirements, the need for international agreements between coalition partners will continue to remain a challenge for policy makers and warfighters. The battlefields of Afghanistan are not the only location where the need for working together as a coalition exists. On December 25th, 2009, an al-Qaeda operative from Nigeria almost detonated plastic explosives on Northwest Airlines Flight 253 from Schiphol Airport in Amsterdam, Netherlands, to Detroit. The New York Times quoted President Barack Obama saying "This was not a failure to collect intelligence; it was a failure to integrate and understand the intelligence that we already had."[25] The failure was in integrated information on hand by other nations, which was not shared with the United States due to the security concerns. The United States will not continue to allow an atmosphere of status quo and limited information sharing that allows potential terrorist cells to grow stronger.[26]

Guidance from the Department of Defense aligns with the need to remove barriers to effective information sharing, adding a special focus area (#5) to its 2009

Information Sharing Implementation Plan to reduce improper and over-classification of information, since those actions "undermine the nation's safety and security by impeding timely sharing of perishable information with relative stakeholders, including…coalition partners."[27] The Implementation plan also states that currently fielded technologies, processes, governance, and policies are not meeting the needs of combatant commanders for mission partner information sharing, and tasks the Defense Information Systems Agency to "Develop an architecture to converge the multiple secret-level coalition networks into a single mission partner assured information sharing environment…"[28]

The creation of international agreements between coalition partners is difficult and time consuming work, and does not support rapid modifications. Even between closest allies, the deliberations between countries can slip from negotiating win-win solutions to the prisoner's dilemma of not cooperating even when it is in the nation's best interest to compromise. The United States may want to limit information sharing to relevant geographic information where the partner nation may want access to theater level readiness information. Conversely, the United States may want unlimited access to sensors managed by a coalition partner, yet the partner may only be willing to share a portion of the data, rather than the information directly from the sensor. International agreements are in place for habitual coalition partners (such as NATO partners or Australia), but may not be in place in sufficient detail with emerging partners (such as other Global Counterterrorism Task Force nations) to provide adequate information sharing on local force protection issues.

Leaders must balance the consistent drive to improve information sharing with equally persistent needs for information security. On a shared battlefield, the United States must trust Coalition partners enough to share information, yet limit the probability of exposure of the information to adversary forces. Although the United States and the European Union have learned the horrors of not sharing information on suspected terrorist personnel and their potential effects on human lives, the duo has "yet to negotiate, draft, and sign a binding international agreement that will govern the sharing of personal information for law enforcement purposes."[29] This leaves both participants open to additional risk for missing key information and possibly stopping a future terrorist event.

The Department of Defense provides some guidance for commanders in time of war or conflict when there is an immediate need to alter information sharing agreements. The Secretary of Defense delegates to the Chairman of the Joint Chiefs of Staff (CJCS) the authority for "agreements for cooperative or reciprocal operational, logistical, training, or other military support…for agreements concerning operational command of joint forces."[30] The CJCS delegates to Overseas Unified Commanders the authority to negotiate and conclude international military telecommunication agreements with coalition partners when such arrangements are in the national interest.[31] This delegation empowers commanders such as the CENTCOM Commander to negotiate an agreement when needed as coalitions add new partners to the effort. While subordinates generally see empowerment as positive since it allows for faster decision making, there could be long-term consequences if forces share the wrong information (such as equipment capabilities or readiness information of other coalition partner) with

a troop contributing nation in the quest to solve operational issues without a true analysis of the strategic importance tradeoffs.

Ongoing Efforts

As technology has improved over the last twenty years, the Department of Defense has continued to improve its capability for information sharing with coalition partners. Each of these activities continues to learn from coalition exercises and operational experiences, working to develop the best product for the Joint Warfighter. The Afghan Mission Network currently provides the best system as a baseline to develop future networks to enable secure information sharing.

As the coalition formed in Afghanistan to defeat Al-Qaeda in support of Operation Enduring Freedom, interoperability concerns required implementation of new processes and agreements to synchronize operations and rapidly share information. In one battle, in Marjah, Helmand Province, Afghanistan, there was a NATO Corps, a British Division, a United States Marine Corps Brigade and a United States Army Brigade all in the same fight, with the tactical requirement to share a common operational picture of the tactical fight.[32] Commanders can enable coordination by exchanging of liaison officers or loaning radio equipment, but the ongoing coalition demonstrations and today's Network Centric Warfare[33] has developed the technical ability to share much more, such as by common operational picture or collaborative planning and discussions. Although the United States had learned some lessons on interoperability from ongoing demonstrations and previous conflicts in Kosovo and Iraq, methods such as providing U.S. coalition partner United Kingdom with U.S. Force XXI Battle Command Brigade and Below (FBCB2) system for combat operations would not be feasible for combat operations in Afghanistan across 40+ coalition partners.

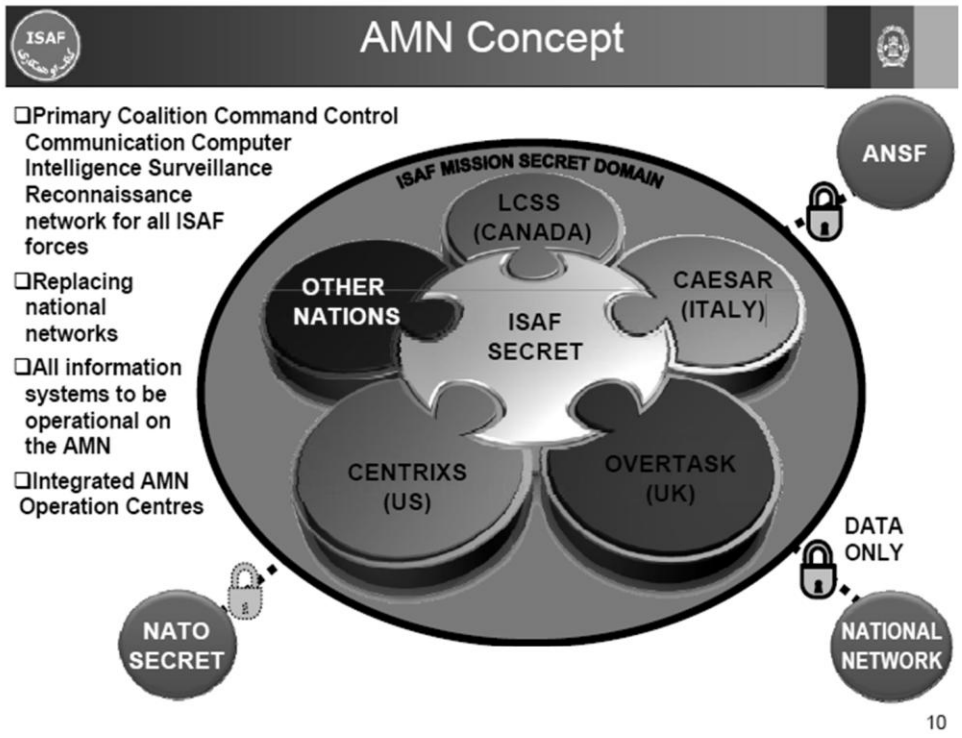

Figure 1. Afghan Mission Network Concept[34]

To meet this interoperability need, the Commander of ISAF required a change in culture to make communications of a Coalition network the norm and acquire a capability "to effectively mix United States and Coalition formations within the Regional Command's battle space - down to Company level"[35] The emerging AMN would merge multiple networks, and include applications in areas such as intelligence, special operations, NATO, medical, and logistic networks to create the ability to share the relevant mission command information across the coalition. The network would not necessarily provide new capabilities to forces (such as provide automated fire control to forces who still use radio based methods), but would rather provide the situational awareness of friendly and enemy force dispositions, locations for critical supplies,

thereby providing the ability to better synchronize coalition combat operations. As the system matures over time, the system would remain flexible to include rapid task organization changes, additional nations as they join the coalition, and serve as the basis for a network that would operate outside the Afghan theater.

Assessment of Risk

As the United States continues operations in Afghanistan and looks into the future to prepare for potential coalition operations beyond 2011, there is a need to assess the risk of whether current coalition mission command efforts are sufficient, and if found insufficient, which areas the United States government should emphasize in a resourced constrained environment. Adapting the five-point model from the February 2008 US IC Information Sharing Strategy assesses the feasibility for the current Afghan Mission Network to serve as the foundation coalition mission command capability for Operation Enduring Freedom in Afghanistan and for future coalition mission command requirements. These assessments lead to specific recommendations to resolve shortcomings and improve future operations.

Consideration 1. Governance. Does the AMN have effective governance and leadership to drive effective and secure sharing of information across coalitions?

Answer. Yes. The leadership and governance for the AMN does not begin at the communications and electronics community and their desire more efficiency in passing data, but rather from the operational community who desire more effectiveness. Technical implementation of the AMN may be in the hands of businessmen and engineers, but leadership of the operational implementation of AMN resides at the senior leadership level in NATO and ISAF/CENTCOM. These senior leaders understand the critical need for security across the coalition, and see the AMN as the

next phase in implementing a solution across tactical and operational communications between troop contributing nations. Agencies outside of CENTCOM also support the AMN. In DISA, the MNIS Program Management Office is leveraging the success of AMN to create more robust systems for use outside the Afghanistan Theater of Operations. NATO supports the AMN as the "primary Coalition Command Control Communication Computer Intelligence Surveillance Reconnaissance network"[36] for all their contributed forces to ISAF. Additionally, Congress has continued to support financially the initial delivery of the system in the Department of Defense's role to disrupt al Qaeda and the Taliban's use of cyber space.[37]

Risk. Low. There is a low risk of the AMN meeting its governance criteria since this program has tremendous leadership involvement and the stakeholders continue to support the system as it develops additional capabilities. Involved coalition partners see the value of the system and have agreed to the policies required for access, but risk can increase when leaders grant expanded access to networks. In such instances, the ISAF Communications section would need to frame the issue for ISAF leadership and try to reach a negotiated agreement, mainly tied to international agreements. Another area could be organizations with atmosphere's that overstress punishment due to exposed information, leading to over-classification of documents. One example is the marking of entire briefings on AMN as "NOFORN" (Not Releasable to Foreign Nationals), when the only one slide may be unsuitable for releasable to warfighters outside U.S. forces. Furthermore, since the AMN program requires additional funding to achieve a full operational capability, there is increased risk that leaders may withdraw support and invest in other capabilities.

Consideration 2. Policy. Are there sufficient policies and standards to guide the balance of sharing information with the security concerns?

Answer. No. This is the area of greatest concern for the future of the AMN and other efforts. Current policies nested in various United States Government strategy documents (such as the National Strategy for Information Sharing or the Information Sharing Strategy) and Department of Defense publications (such as DoD Plan or Joint Publication 2-0 on Joint Intelligence) do not provide enough detail on the balance between security and information sharing. In general, these documents are strong with regard to removing barriers and increasing sharing with coalition partners, leaving the decision on how much to share in the gap created between the international agreement and the rapid analysis of the Combatant Commander. Unfortunately, international agreements take too long to initiate to match the fast flowing changes in both technology and task organization on the battlefield. In addition, Combatant Commanders may err on the side of overcoming operational issues and winning tactical battles, without sufficient analysis of second order efforts to strategic issues. An example includes sharing the video feed between United States forces and Coalition partners to overcome the advance of enemy forces. If the coalition partner does not have adequate protection from hackers, or protection from internal misuse of classified material, such video could inform enemy forces on the capabilities of United States assets, altering enemy procedures and reducing the tactical advantage of United States equipment. Although the AMN's architecture requires a conscious decision on what operators tag and post information to the shared data environment, the lack of technical guidance on potential compromises to current capabilities on information sharing could

hinder future operations. Current capabilities documents that guide future technical solutions for the long-term coalition data environment assume adequate time to initiate coalition based networks, which represents the obsolete idea of a Cold War or Desert Storm buildup phase to operations, rather than rapid transitions from Phase Zero Shaping Operations to Phase III Dominate (Combat Operations).[38]

Risk. High. Even with significant advances in technology, there is a high probability that operators will improperly share information across a coalition network, and there is likely a moderate negative consequence based on the shared information. Brigadier General Susan Lawrence, while she was commander of the U.S. Army Network Enterprise Technology Command/9th Signal Command, stated that “Our enemies are all over the network."[39] Although this focused on the garrison based network, the same desire applies to United States combat networks. Without additional policy guidance to address the rapid creation of coalition networks, commanders will continue to face elevated risk when pressed with sharing classified information with coalition partners.

Consideration 3. Technology. Is the technology in place to enable effective and secure sharing across the coalition?

Answer. Initially - Yes. This is a great developing strength of the AMN. Multiple Army Acquisition organizations came together and took the best ideas from the multiple coalition information sharing systems across to work with NATO to develop the AMN. [40] The system provides the common core ISAF Secret network that participating coalition partners can securely tie into the network interconnection points without fear of undue exposure to host nation systems, such as the United States Combined Enterprise

Regional Information Exchange System (CENTRIXS). There are common data standards for participants to organize, indentify, and search for information. Participants can push information to the core domain and pull information from other participating sources. Administrated control access to the network through country based user interfaces, and country network administrators can audit system usage to ensure only valid participants access the core, without infringing into the sovereignty of the coalition partners host system.

Risk. Moderate. Although the ISAF Secret network provides the screening at the nation level, the limit of not automating control at the user level could lead to security concerns due to a perceived lack of individual accountability. The risk for individuals to violate security protocols and have information become visible to unauthorized viewers is low-moderate, and this can become moderate to high as technology unfortunately develops measures to avoid security protocols. Where unsecure networks hosted on the World Wide Web are more susceptible to hackers and data loss, this network begins with a secret framework, with a general expectation of trusted viewers. The risk becomes more moderate as coalition partners become interested in data about other troop contributing nations, specifically nations that may be adversaries or unfriendly outside the Afghanistan Theater. Other technology risks include the rapid need to modify sharing permissions with coalition partners based on short-term tactical needs, such as short-term access to unmanned aerial vehicle (UAV) video, without truly assessing the cost of acknowledging such capabilities to the partner coalition troop contributing nation. An example of this would be sharing video from a high altitude UAV to synchronize effort and counter an imminent threat, exposing the

capability for such UAVs to operate in the local conditions. One area that can continue to develop is the ability for information sharing across multiple languages, rather than only provided in English. In addition, there always remains a minor risk that a network user may place un-authoritative data (such as a position or weather estimate rather than actual data) on the network and another user may mistakenly make an incorrect decision based on that data.

Consideration 4. Culture. Does the culture of the users of coalition mission command information support securely sharing information across the network?

Answer. No. This area is improving, but not fully developed. Certainly the United States Armed Forces have learned from the lessons of Desert Storm and Kosovo the need to share information and have made great progress in the area. Providing the equipment to ensure sharing is insufficient. The 21st century technology involved with Network Centric Warfare has developed the ability to share much more than voice commands over a shared radio or paper files across Liaison officers. The leadership involvement from both ISAF and CENTCOM has helped expand the culture of sharing over the almost ten years of conflict in Afghanistan. This motivates users to share data across the network, seeing the value from the synergy of pooling information on known or suspected enemy locations to enable more productive attacks or tie together information on terrorists to locate hideouts and leader locations. The decisions on what information to place on the core ISAF network remains empowered to the originating source, but likely routine coalition communications meetings and training enable participants to voice concerns over any concerns over insufficient sharing arrangements. Additionally, with the global issue caused by the unauthorized document

release from Wikileaks, organizations may revert to more closed societies and share less information.

Risk. Low. The will to share will improve as partners continue to work together, keeping the risk low at cultural barriers impeding coalition information sharing. ISAF partners have overcome the initial cultural barriers over the past decade, and continue to emerge new approaches as technology enables faster downloads of information and increased bandwidth for sharing of graphics and video. There will also remain the risk of counterintelligence, which leaders must consider in coalition operations.

Consideration 5. Economics. Are there sufficient resources to enable secure information sharing?

Answer. Initially Yes. With both the United States providing an approximate $100M initial investment and NATO proving an additional $15M to improve the ISAF Secret Network[41], there have been sufficient resources infused into the AMN to provide a base for information sharing. Over time, multiple programs have spent resources to ensure their data can traverse the AMN, which may include rewriting software code to enable sharing outside the United States CENTRIXS.

Risk. Moderate. Although NATO and the United States adequately funded the initial capability of the AMN, there remains an annual funding requirement for ongoing operations and maintenance, which competes each year with other priorities in budgets. Also, as commanders deem information sharing more valuable, there is a moderate risk that system users will want enhanced capabilities, such as additional bandwidth or faster download speeds, which will require additional investments. This risk is greater for the United States, which has a larger leadership role in ISAF than other nations,

although there will continue to be shared risk for each troop contributing nation to improve their user terminals to accept the information provided over the AMN. One resource that will continue to be challenging is user training time. As new coalition partners join the AMN, there is a need to simplify the process to join the AMN, train users of the systems on how to organize and search for information, and find ways to push information to other AMN participants.

Recommendations.

Based on the five considerations derived from the United States Intelligence Community model, participants in the information sharing community can improve each area of governance, policy, technology, culture, and economics. Through a combination of improvements in technology and guidance, the United States Government can enhance the AMN and future coalition networks to better handle the challenge of balancing sharing information across the coalition with maintaining the security protocols to ensure national security.

Recommendation 1. Governance. To continue to ensure the AMN retains effective governance and leadership to drive effective and secure sharing of information across coalitions, CENTCOM and ISAF leaders need to continue strategic communication with network participants. This consistency becomes increasingly relevant as military leaders of organizations change over time more frequently than civilian counterparts. DISA should continue to provide updates through CENTCOM on the transition from a product focused on Afghanistan to a more deployable system, able for rapid installation regardless of theater of operation. ISAF should continually seek feedback from coalition partners on usage and future developmental needs, and document changes made due to tactical expediency of battlefield operations into

international agreements. As long as organizations (such as NATO and the United States) work together and not compete for the leadership role in this effort, the AMN can continue to provide effective information sharing across the coalition.

Recommendation 2. Policy. Applicable policymakers should modify current policies to address the rapid decision making required by Commanders over the need to share information, and the potential effects. The revision of Department of Defense Directive 8320.2 should include guidance on levels of information sharing based on time constraints, current theater operations, and future tactical confrontations. Joint Publication 6-0 (*Joint Communications*) should expand the guidance provided to foreign disclosure officers on tiered level of information releasability that is situational dependant rather than an "all or nothing" approach. The DoD Information Sharing Implementation Plan and Joint Publication 2-0 (*Joint Intelligence*) should include additional guidance to assist commanders to make rapid decisions on information sharing, such as case scenarios as commanders form new task organizations in forward operating basis or as coalitions add new partners to emerging combat operations. If possible, nations should craft international agreements giving maximum flexibility to commanders, stressing only the limits of what not to share (such as key technologies, peer capabilities, etc.) rather than prescribe what information can be shared (such as common terrain products, electronic mail, etc.). Although policy changes alone will not improve information sharing, they provide the foundation for improved decision making for commanders faced with balancing information security and sharing requirements. This recommendation realized the danger that too much policy restricts the ability for commanders to make flexible decisions on the battlefield to

overcome emerging challenges, so policymakers must use caution not to limit commanders beyond the requirements of law or statute.

Recommendation 3. Technology. CENTCOM/ISAF should continue periodic infusion of well tested technology to improve incrementally secure information sharing across the coalition. Upgrades in both the software managing sharing permission and the training of coalition partners on the use of the AMN can continue to improve the technologies ability to balance security and information sharing. Future integration of language independence or easily translated software can help coalition partners better understand the mission command information. In addition, the software requires improvements in technology to counter emerging threats from future hackers, who may capture or decrypt weaker coalition partner security systems. Continue to enhance the ability of the coalition network to handle additional data and information bandwidth, and integrate advances in communications technologies to improve system reliability and user interfaces. The Department of Defense should continue to manage efforts to develop and field additional capability as acquisition programs of record, to ensure adequate testing of security and interoperability. In parallel, additional capability will require additional training, which the Army should integrate into initial entry and follow on courses taken at Training and Doctrine Command schools.

Recommendation 4. Culture. Continue to stress the importance of coalitions and cultural awareness, and emphasize the importance of trusting coalition partners with appropriate information. Encourage coalition partners to continue to populate shared environments with relevant information. Overcome negative media related to released

classified information due to Wikileaks or other sources, and celebrate successes in sharing information that lead to battlefield victories.

Recommendation 5. Economics. Market successes in the AMN to key stakeholders to include Congress and Department of Defense leadership, to ensure continued funding in maintenance of current systems and development of future systems. Invest as soon as possible for the next generation of the AMN, developing into a system that incorporates other coalition lessons learned from the USEUCOM Battlefield Information Collection and Exploitation Systems program and the variant of the Global Command and Control System used in Korea. Re-evaluate the need for multiple versions of coalition information sharing systems focused on geographic areas, and develop one modular system capable of integration of any coalition partner regardless of hardware. Understanding systems may require minor adjustments to hardware, but open systems architecture and non-proprietary software will reduce rework needed for future coalition partners to join United States involved networks. One caution is the realization that as NATO and the United States reduces its involvement in the coalition in Afghanistan, Congress and other financial organizations may reduce funding from Defense spending to other national needs. To prepare for follow on conflicts, acquisition organizations should pool resources and work together to continue to improve from the foundation of the AMN and reduce the network construction time for follow on operations. Acquisition Program Managers and writers of system requirements should anticipate the need to modify ongoing and future systems to allow for better integration into coalition networks.

Conclusion.

While commanders adequately balance information sharing and security each day through their dedicated intelligence, communications, and foreign disclosure officers, improvements to published guidance and technology can reduce risk and preserve United States combat advantages. As President Barack Obama states in the Introduction of the 2010 National Security Strategy, throughout history the United States have operated with coalition partners to win World War II and end the Cold War, and in the future, the United States will continue strengthening coalition alliances to achieve national objectives.[42] The Department of Defense has several ongoing efforts in information sharing, highlighted by the success with the AMN used in Operation Enduring Freedom. Although the AMN provides a significant improvement over historical methods of coalition information sharing, and has significant leadership support for the product and culture of sharing, there is need to revise existing Department of Defense guidance to support the rapid requirements of Combatant Commanders. With adequate funding, technology can provide some resolution of ongoing issues, but follow on conflicts may not allow the eight year learning curve seen in Afghanistan to ensure coalition partners can securely share information at the start of operations.

Endnotes

1 Barack H. Obama, *National Security Strategy* (Washington, DC: The White House, May 2010), 41.

[2] Robert M. Gates, *National Defense Strategy* (Washington, DC: Department of Defense, June 2008), 8.

[3] Ibid., 21.

[4] U. S. Department of the Army, “Enhancing International Security Assistance Force Preparation,” *Stand-To!,* May 14, 2010, http://www.army.mil/standto/archive/2010/05/14/ (accessed October 27, 2010).

[5] U. S. Joint Chiefs of Staff, *Joint Intelligence*, Joint Publication 2-0 (Washington, DC: U.S. Joint Staff, June 22, 2007), 110.

[6] U.S. Government, Coalition Management, Strategic Plans and Policy Directorate Manual J-5M 2350.01, July 5. 2006, unclassified excerpt of the National Strategic Plan for the War on Terrorism, Annex G, 4 March 2005. A-D-1. http://jcs.dtic.mil/j5/ coalition_ management.pdf (accessed October 27, 2010.)

[7] George W. Bush, *National Strategy for Information Sharing* (Washington, DC: The White House, October 2007), 1.

[8] Ibid., 4.

[9] Ibid., 25.

[10] Clay Wilson, Network Centric Warfare: Background and Oversight Issues for Congress. *Congressional Research Service* (Washington, DC: The Library of Congress, June 2, 2004), 26, http://fpc.state.gov/documents/organization/33858.pdf (accessed November 3, 2010.)

[11] John M. McConnell, *Information Sharing Strategy* (Washington, DC: U.S. Intelligence Community, February 22, 2008), 8.

[12] Ibid., 15.

[13] Robert M. Gates, “Letter to Senator Carl Levin,” U. S. Secretary of Defense. August 16, 2010, http://www.fas.org/sgp/othergov/dod/gates-wikileaks.pdf (accessed October 27, 2010.)

[14]Theresa A. Pardo and G. Brian Burke, *Government Worth Having: A Briefing on Interoperability for Government Leaders,* Center for Technology in Government: University at Albany, State University of New York, October 21, 2008, 8, http://www.ctg. albany.edu/publications/reports/government_worth_having/government_worth_having.p df. (accessed October 27, 2010.)

[15] U.S. Joint Chiefs of Staff, *Joint Communications System,* Joint Publication 6-0 (Washington, DC: U.S. Department of the Defense, June 10, 2010), III-8.

[16] U.S. Joint Chiefs of Staff. *International Military Agreements for Rationalization, Standardization, and Interoperability Between The United States, Its Allies, And Other Friendly Nations*, CJCSI 2700.01C (Washington, DC: U.S. Department of the Defense, February 8, 2008), A-1.

[17] John Aclin, “Intelligence as a Tool of Strategy.” In U.S. Army War College Guide to National Security Issues 4th edition. Volume 1. Theory of War and Strategy, J. Boone Bartholomees (Carlisle Barracks PA: Strategic Studies Institute US Army War College, July 2010), 274.

[18] United States Department of Defense, “Quadrennial Defense Review Report” February 2010. http://www.defense.gov/qdr/images/QDR_as_of_12Feb10_1000.pdf (accessed January 6, 2011), 90.

[19] Brigadier General Brian J. Donahue, *Afghan Mission Network*, U.S. Central Command presentation at Landwarnet 2010, August 3, 2010, http://www.afcea.org/events/ landwarnet/10/videos/track1/LWN2010%20Track%201%20Session%203.wmv (accessed October 27, 2010.)

[20] U.S. Joint Chiefs of Staff. *International Agreements,* CJCSI 2300.01d (Washington, DC: U.S. Department of Defense, October 5, 2007), C-1. These agreements may be regionally specific or focused on individual conflicts.

[21] U.S. Joint Chiefs of Staff, *Information Operations*, Joint Publication 3-13 (Washington, DC: U.S. Department of the Defense, February 13, 2006), VI-2.

[22] Henry S. Kenyon, “Information Sharing Crucial to Asian Operations,” *Signal Online Magazine*, October 2008, http://www.afcea.org/signal/articles/anmviewer.asp?a=1715&print=yes, (accessed October 27, 2010.)

[23] Barry Rosenberg. “Can you hear me now? How To Stay Connected In Afghanistan. WIN-T Project Manager Faced Political and Technical Problems in Theater”, *Defense Systems*, Oct 12, 2010, http://defensesystems.com/Articles/2010/10/15/Lessons-Learned-Warfighter-Communications-in-Afghanistan.aspx?Page=1, (accessed October 27, 2010.)

[24] Lieutenant Commander Mark A. Nicholson, “Piecing Together the Network-Centric Puzzle: Using Operational Functions to Analyze Potential Coalition Partners”, *Joint Military Operations Department* (Newport, RI: Naval War College February 15, 2005), http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA464306, (accessed November 3, 2010), 3.

[25] Jeff Zeleny and Helene Cooper, “Obama Says Plot Could Have Been Disrupted,” *New York Times*, January 5, 2010, http://www.nytimes.com/2010/01/06/us/politics/06obama.html (accessed October 27, 2010.)

[26] Derek S. Reveron, “Old Allies, New Friends: Intelligence-Sharing in the War on Terror,” *Orbis*, Summer 2006, 3.

[27] U.S. Department of Defense, *DoD Information Sharing Implementation Plan,* (Washington, DC: U.S. Department of Defense, April 2009) 19.

[28] Ibid., 18.

[29] Hiroyuki Tanaka, Rocco Bellanova, Susan Ginsburg, and Paul De Hert, *Transatlantic Information Sharing: At a Crossroads,* Migration Policy Institute, January 2010, 4, http://www.migrationpolicy.org/pubs/infosharing-Jan2010.pdf, (accessed October 27, 2010.)

[30] U. S. Department of Defense, *International Agreements*, DoD Directive 5530.3 (Washington, DC: U.S. Department of Defense, February 18, 1991), 14-15.

[31] U.S. Joint Chiefs of Staff, *Military Telecommunications Agreements and Arrangements between the United States and Regional Defense Organizations or Friendly Foreign Nations*, CJCSI 6740.01B, (Washington, DC: U.S. Department of Defense, March 28, 2008), A-3.

[32] Brigadier General Brian J. Donahue, *Afghan Mission Network*.

[33] Vice Admiral Arthur K. Cebrowski, USN, and John J. Garstka, "Network Centric Warfare: Its Origin and Future," Proceedings of the Naval Institute 124:1 (January 1998): 28-35.

[34] Dag Wilhelmsen, “Afghanistan Mission Network (AMN) in Operational Environment.,” briefing slides, Koblenz, Germany, NATO CIS Services Agency, September 2, 2010, http://www.afcea.de/fileadmin/downloads/Fachtagung/Koblenz_ 2010/ 6%20Wilhelmsen%20-%20(NU)%20NCSA%20TD%20Presentation%20to%20 AFCEA%20Koblenz% 20020910%20final.pdf, (accessed December 2, 2010,) 10.

[35] Brigadier General Brian J. Donahue, *Afghan Mission Network.*

[36] Ibid.

[37] General Keith Alexander, *Cyberspace Operations Testimony,* House Armed Services Committee, Washington, D.C., September 23, 2010, http://www.stratcom.mil/ speeches/52/House_Armed_Services_Committee_Cyberspace_Operations_Testimony (accessed December 2, 2010.)

[38] U. S. Department of Defense, *Joint Operation Planning*, Joint Publication 5-0 (Washington, DC: U.S. Chairmen of the Joint Chiefs of Staff, December 26, 2006), IV-35.

[39] Brigadier General Susan Lawrence, as quoted in “Information Sharing Challenges on a Multinational Scale” MITRE, September 2008, http://www.mitre.org/ news/digest/defense_intelligence/09_08/multops.html (accessed December 8, 2010).

[40] Harrison Donnelly, “Fielding Networked Battle Command Solutions - Q&A: Brigadier General N. Lee S. Price,” *Military Information Technology*, October 2010, http://www.kmimediagroup.com/files/MIT_14-9_final.pdf (accessed December 2, 2010).

[41] Ibid.

[42] Barack H. Obama, *National Security Strategy, 41*.