CANADIAN FORCES COLLEGE / COLLÈGE DES FORCES CANADIENNES
CSC 31 / CCEM 31

MDS

Multinational Knowledge-sharing

By Major Stan (Scott) Diamanti

TABLE OF CONTENTS

LIST OF FIGURES

ABSTRACT

Modern warfare has created a greater dependency on information systems to provide political and military leaders with the knowledge necessary to aid in the decision-making process. Taken in the context of multinational operations, in which forces have varying degrees of information systems and knowledge sharing capabilities, friction between systems and capabilities can hamper effective decision-making. Therefore, it is incumbent upon all nations seeking multinational support to develop knowledge sharing systems to counteract the effects of friction to multinational operations.

Interoperability is the first of three key determinants to effectively implementing knowledge sharing. Personnel and systems must initially have the capacity to exchange knowledge before they can begin to realize the advantages provided by knowledge sharing. Language and standardized terminology is another key aspect, in which the establishment of liaison officers with both linguistic skill and area knowledge is the tried and true approach to ensuring that knowledge is effectively transferred between nations. The last determinant is the ability to release certain aspects of secure information. The protection of information sources is so great, that in many cases nations fail to pass critical decision-making knowledge in a timely fashion.

With superior information comes superior knowledge and with superior knowledge sharing comes superior multinational decision-making. By effectively developing knowledge sharing systems that are interoperable, take into account language differences, and allow various levels of access, nations can provide both political and military leadership the necessary information required for decisions.

SECTION 1

INTRODUCTION

> "The only thing in war worse than having to fight with allies is having to fight without allies."
> - Sir Winston Churchill, WWII

"The United States remains the prime guarantor of Western security, especially in protecting common interests outside Europe. In the future, however, the task of sustaining this burden single-handedly is likely to become increasingly difficult for the United States for both economic and political reasons."[1] For this reason, this paper assumes that most military operations in the future will more than likely be conducted by multinational forces, whether it is under the auspices of the United Nations (UN) or North Atlantic Treaty Organization (NATO) or just a coalition of the willing. However, anytime nations combine efforts to counter a perceived common threat, problems may arise. For alliances, "the more extensive the threat, the easier it is to narrow the gap [such as member state differences]; the less extensive or dangerous, the more likely the allies are to risk intra-alliance friction in order to attain their own goals."[2] From political differences to military strategy and security of national knowledge, all may well play a role in creating friction for allied forces. These same problems are equally evident, if not amplified, when operating in a loosely linked, ad hoc coalition environment. To

---

[1] Richard Sokolsky, Stuart Johnson, and F. Stephen Larrabee, *Improving Allied Military Contributions* (Arlington, Virginia: Rand Corporation, 2000), xiii.

[2] Robert L. Rothstein, *Alliances and Small Powers* (New York, New York: Columbia University Press, 1968), 59.

counteract the effects of friction caused by multinational operations, nations must pursue knowledge-sharing systems that create opportunities for member states to provide effective military contributions to combined operations. To this end, the paper will conclude that system interoperability, language, and the release of secure national information are the three key determinants for effectively developing systems capable of adequately sharing knowledge amongst multinational forces.

This document will first evaluate the reasoning behind and composition of alliances and coalitions. Upon explanation of the various multinational configurations, the paper will provide a common understanding of the three key determinants of knowledge sharing. From these descriptors, the author will examine two historical alliances and the current coalition conducting Operation Iraqi Freedom, for evidence of the three key determinants to ascertain their contribution either to the success or failure of the multinational campaign.

By understanding the historical problems associated with forces attempting to share knowledge, focus can then shift to the potential benefits associated with effective knowledge sharing. By illustrating the effects knowledge sharing can make on the dissemination of critical information to operational and tactical multinational forces, the acceleration of the decision-cycle made by all multinational members, and the common situational awareness knowledge sharing can provide, it should be evident to the reader the need to advocate knowledge sharing implementation. To contrast the benefits of knowledge sharing, this paper will investigate the major challenges to implementing knowledge-sharing systems and what potential opportunities exist to mitigate the risks or barriers associated with each concern.

After defining both the benefits and challenges of knowledge sharing, attention will move to the understanding of knowledge sharing process itself. Initial research will focus on data and its transformation to information and then into knowledge. After knowledge is extrapolated, then it will be critical to explain the importance of dissemination, which in-turn can enable highly effective multinational knowledge sharing. In the process of analyzing the path of knowledge from data to the decision-maker, it will be critical to equally examine the need for a common infrastructure and more specifically the approach used by the United States. However, hardware alone cannot bring about the transformation of data into knowledge; therefore, the document will evaluate current and projected major U.S. and international acquisition initiatives or concepts designed to enhance knowledge sharing and effectiveness of multinational partners in the theater of operations.

Upon conclusion of this document the reader will have a clear understanding of the importance of the implementation of knowledge sharing systems. By illustrating how the benefits of knowledge sharing far outweigh the roadblocks, coupled with the identification of synergies that can be created by developing systems jointly and within the context of operating as a multinational force, it will be abundantly clear to the reader the need to advocate development of knowledge-sharing systems. Ultimately, it is in the interests of all nations seeking multinational support to pursue common knowledge-sharing systems that provide interoperability, a common language or understanding of terminology, and adequate intelligence access and security.

SECTION 2

MULTINATIONAL OPERATIONS

> **"People everywhere want to be able to speak freely; choose who will govern them; worship as they please; educate their children—male and female; own property; and enjoy the benefits of their labor. These values of freedom are right and true for every person, in every society—and the duty of protecting these values against their enemies is the common calling of freedom-loving people across the globe and across the ages."**
>
> **- President George W. Bush, The National Security Strategy of the United States of America, 2005**

"'Multinational operations' is a collective term to describe military actions conducted by forces of two or more nations."[3] Traditionally, nations have sought multinational support for operations because they "…afford political legitimacy (e.g., through United Nations Resolutions), and can ease domestic objections to military operations."[4] In seeking potential partners for multinational operations, nations may use political or ideological similarities, religious or ethnic similarities, economic interdependencies, or a host of other influences to gain support for their objectives. However, "Cultural, psychological, economic, technological, informational, and political factors as well as transnational dangers all impact on multinational operations."[5] In the end, "Nations come together in multinational operations because of their own security

---

[3] Joint Chiefs of Staff, *Joint Publication 3-16: Joint Doctrine for Multinational Operations* (Washington, D.C.: U.S. Government Printing Office, April 2000), I-1.

[4] Eric S. Miller, "Interoperability of Rules of Engagement in Multinational Maritime Operations" (Center for Naval Analyses Research Memorandum, October 1995), 11.

[5] Joint Chiefs of Staff, *Joint Publication 3-16: Joint Doctrine for Multinational Operations*, I-2.

interests, although the specific objectives do not necessarily have to coincide."[6] In other words, a nation will join a multinational operation only if the nation perceives the operation as within national interest. "Where commonality or compatibility of interest exists, nations may enter into political, economic, and military partnerships."[7]

Multinational operations "…are usually undertaken within the structure of a coalition or an alliance, although other possible arrangements include supervision by an international organization (such as the United Nations (UN) or Organization for Security and Cooperation in Europe)."[8] An alliance is "a relationship between countries or organizations for a joint purpose,"[9] or a "formal arrangements between two or more nations for broad, long term objectives."[10] Upon entering an alliance, nations may be required to dismiss specific individual national rights in support of allied objectives. "A formal tie [between nations] may be accepted in hopes of gaining the right to be consulted."[11] Consultation between member states of an alliance "…are one of the primary means by which states seek the co-operation of other states in order to enhance their power to protect and advance their interests."[12] In some instances states may join an alliance to counter potential offensive action by neighboring nations. In such a case,

---

[6] Eric S. Miller, "Interoperability of Rules of Engagement in Multinational Maritime Operations," 10.

[7] Joint Chiefs of Staff, *Joint Publication 3-16: Joint Doctrine for Multinational Operations*, I-2.

[8] *Ibid.,* I-1.

[9] Catherine Soanes, *Pocket Oxford English Dictionary,* 9th ed. (Oxford, New York: Oxford University Press, Inc., 2002), *22.*

[10] Joint Chiefs of Staff, *Joint Publication 3-0: Doctrine for Joint Operations*, VI-1.

[11] Robert L. Rothstein, *Alliances and Small Power*, 49.

[12] Robert E. Osgood, *Alliances and American Foreign Policy* (Baltimore, Maryland: The John Hopkins Press, 1968), 17.

"one might also ally in order to use the alliance as a bargaining weapon against another power, offering to dismantle the new alliance in exchange for certain stipulated responses."[13]   Whatever the circumstances of the situation, "It is safe to assume that most allies seek both political and military advantages from any alliances."[14]

> "To win a battle by fighting is not the best strategy; to conquer the enemy without having to resort to war is the highest, most admirable form of generalship. The next best form of generalship is to conquer the enemy with an alliance - by borrowing strengths from one's allies." - Sun Tzu, The Art of War

One example of an alliance relationship is that of the North Atlantic Treaty Organization (NATO). Following World War II, the Soviet Union began to emerge as a potential threat to the prosperity of both European nations and those of North America. To equalize this potential threat Belgium, Canada, Denmark, France, Iceland, Italy, Luxembourg, Netherlands, Norway, Portugal, United Kingdom and the United States entered into "…a single North Atlantic Alliance based on security guarantees and mutual commitments."[15] Since the 1949 agreement Bulgaria, the Czech Republic, Estonia, Germany, Greece, Hungary, Latvia, Lithuania, Poland, Romania, Spain, Slovakia, Slovenia, and Turkey have become members of NATO. All contributing to common effort "to deter and defend against any threat of aggression against any NATO member state."[16]

---

[13] Robert L. Rothstein, *Alliances and Small Powers*, 50.

[14] *Ibid.*, 50.

[15] North Atlantic Treaty Organization (NATO), *NATO Handbook* (Brussels, Belgium: NATO Office of Information and Press, 2001), 29.

[16] *Ibid.*, 32.

So what is a military coalition and how does it differ with respect to an alliance? Oxford's Dictionary defines it as "a temporary alliance,"[17] or as U.S. Joint Doctrine defines it a "…coalition is an ad hoc arrangement between two or more nations for common action."[18] In many situations, there will be differences between nations that preclude the establishment of formal alliances. For instance, because "…of cultural, religious, and political reasons, the United States lacks a formal alliance in Southwest Asia."[19] However in many situations formal alliance agreements may not be required. In cases that warrant only a multinational military response, "…but no alliance exists, a coalition of nations with similar interests is a feasible alternative to resolve the problem."[20] These nations may temporarily enter into agreements to counter a common threat. Equally, in many third world nations, no formal alliances have been established, therefore to "…less-developed countries, any extension of American commitments will almost surely take place chiefly by means other than alliances."[21]

As the authors of *Balance of Power: Theory and Practice in the 21st Century* point out, alliances can be seen as using more "hard balancing" strategies for dealing with rival nations. This hard balancing takes form in "…strategies to build and update their military capabilities, as well as create and maintain formal alliances and counter-

---

[17] Catherine Soanes, *Pocket Oxford English Dictionary,* 164.

[18] Joint Chiefs of Staff, *Joint Publication 3-16: Joint Doctrine for Multinational Operations*, vii.

[19] Colonel William H. Parry, III, "Multinational Operations and the National Security Strategy: The Modern Melian Dialogue" (United States Army War College Strategy Research Project, 2000), 3.

[20] *Ibid.*, 3.

[21] Robert E. Osgood, *Alliances and American Foreign Policy*, 162.

alliances, to match the capabilities of their key opponents."[22] Coalitions, on the other

hand, tend to focus on the use of soft balancing strategies. In soft balancing, strategies

are "…based on a limited arms buildup, ad hoc cooperative exercises, or collaboration in

regional or international institutions."[23] Although soft balancing or coalitions may

initially be used, there is nothing to preclude the conversion "…to open, hard balancing

strategies if and when security competition becomes intense and the powerful state

becomes threatened."[24]

The notion of balancing raises the important issue of capability. In almost all

instances, alliances and coalitions will include states with very different capability bases.

For alliances this may be more prevalent in "regional" alliances, in which national

capabilities of neighboring countries that are allied vary. For instance, if we look at the

Organization of American States (OAS) we can highlight very different levels of national

capability between the United States and Uruguay.   However, "In the American vision of

international order, multilateral 'regional' alliances have a special place because they

presumably transcend and subordinate separate national interests, represent indigenous

harmony and initiative, and permit the United States to be one among several 'partners,'

even if it is the senior partner."[25] Therefore one can assume that, if necessary, the more

powerful state may be called upon to provide greater capability to support others.

---

[22] T.V. Paul, James J. Wirtz, and Michel Fortmann, *Balance of Power: Theory and Practice in the 21st Century* (Stanford, California: Stanford University Press, 2004), 3.

[23] *Ibid.*, 3.

[24] *Ibid.*, 3.

[25] Robert E. Osgood, *Alliances and American Foreign Policy*, 2.

Likewise, in coalitions, even greater disparity potentially exists between the capabilities of established powerful states and emerging nations seeking international support.

Since there will always be disparity in national capabilities, one can deduce that no matter whether a nation belongs to either a formal alliance or a more loosely linked coalition, the importance and requirements of a knowledge sharing system will remain relatively similar. But how then can one ensure that effective knowledge sharing can take place? There are three key determinants critical to the successful knowledge sharing between nations. The first deals with the interoperability of national and/or international systems. "Not all the member nations in existing alliances will ever be able to match the U.S. technology and industrial bases."[26] Nations with greater communications and information capabilities will need to be prepared to extend this support to multinational partners lacking organic support. "Historically, the problems of interoperability have been solved — when they have been solved at all — primarily through trial and error during actual conduct of operations over an extended period of time."[27] However, unless action is taken to build interoperability with multinational forces into systems, the operational success of a multinational endeavor may be jeopardized by the delay caused in ensuring all forces are able to participate in an integrated fashion. "The most important areas for interoperability include language, communications, doctrine, and exchanges of information."[28]

---

[26] Colonel William H. Parry, III, "Multinational Operations and the National Security Strategy: The Modern Melian Dialogue," 26.

[27] Joint Chiefs of Staff, *Joint Publication 3-16:Joint Doctrine for Multinational Operations*, I-12.

[28] Joint Chiefs of Staff, *Joint Publication 3-16:Joint Doctrine for Multinational Operations*, I-12.

This brings up our second determinant for ensuring effective knowledge sharing, the development of a common language or terminology set or just plain breaking the language barrier. Militaries have traditionally used liaison personnel and/or common repositories of international terminology to bridge some of the language gaps between nations. "Language content is conveyed by word choice, mannerisms, and other means, and information loss, miscommunications, and misunderstandings can have a negative effect on operations."[29] It is imperative that lead nation for multinational operations understand the different linguistic skills, any significant body language cues and potential pitfalls associated with communicating with nations included in specific operations. "Understanding language and culture are key factors to successful liaison operations,"[30] and in-turn, to effective knowledge sharing.

National ability to release classified or secure information to multinational forces encompasses the third determinant of knowledge sharing effectiveness. This is to say that although systems may be interoperable, and nations may have found a common language base to work from, they still must overcome the ability to provide intelligence data to one another. "The sole reason for the existence of the intelligence community exists for the purpose of reducing uncertainty on political and military issues."[31] This is not to say that one nation will be required to provide full access to other nations, just that to ensure all forces are operating in concert, all nations involved in an operation must have access to the same critical information necessary to conduct operations.

---

[29] *Ibid.*, III-13.

[30] *Ibid.*, II-13.

[31] Michael I Handel, *War, Strategy and Intelligence* (London, England: Frank Cass and Company Limited, 1989), 196.

"Ultimately, sharing intelligence information gives everyone the same situational awareness,"[32] and once again enables effective knowledge sharing.

How then is one to be sure that these three determinants are the primary prerequisites for effective knowledge sharing systems? This paper will look at three historical cases of multinational operations and gauge the existence and exercise of the three determinants to determine the success or failure of the campaign.

Auld Alliance

The first multinational campaign for consideration is the Auld Alliance, "The oldest mutual self-defense treaty in Europe,"[33] was between Norway, France and Scotland. "First agreed in 1295/6 the Auld Alliance was built on Scotland and France's shared need to curtail English expansion."[34] During the period of the alliance, over three hundred years, both Scotland and France provided mutual military support when called upon to restrain England's aspirations for sovereignty over both regions.

When it came to interoperability, the Scottish and French were similar to most medieval European forces of the time. Archers and infantry had a role in most battles, but the centerpiece of any military at the time was the cavalry. "So far as the methods of warfare were concerned, there were differences but the constant was the importance of cavalry."[35] To coordinate movement of the different forces, "tactical movements were

---

[32] *Ibid.*, 33.

[33] R.M. Gunn, "William the Lion of Scotland," *AOL.Hometown* (2003); available from http://members.aol.com/skyewrites/thelion.html; accessed 1 February 2005.

[34] British Broadcasting Corporation, "The Auld Alliance – Scotland and France," http://www.bbc.co.uk/history/scottishhistory/europe/features_europe_auldalliance.shtml; Internet; accessed 3 April 2005.

controlled by black and white signal flags under the direction of squadron and regimental commanders."[36] Contacting geographically divided forces would also prove challenging, but most European forces made "…extensive use of couriers for long-range communications purposes."[37] Since most of the forces at the time engaged in similar activities, problems associated with communications interoperability were minimal.

The alliance, although political and military in nature, also "…granted dual citizenship in both countries."[38] This dual citizenship would last until 1905 when France revoked the privilege. "The Auld Alliance influenced everyday life by affecting architecture and even the language [Scottish] people spoke by borrowing French words."[39] Although the difficulty with language was reduced as forces were deployed to alternate countries for long periods of time, during several battles, such as the Battle of Bannockburn, communications between forces would still be prove to be challenging. At the Battle, Sir Robert the Bruce held command of a force consisting of Scottish troops from varying regions of the country. Realizing that languages of the country differed by region and that his "…main numbers of the forces were Highlanders who spoke little to no English or French,"[40] he broke the forces into different groups. Lowland forces mixed

---

[35] Adrian Gilbert, *The Encyclopedia of Warfare From the Earliest Times to the Present Day* (Chicago, Illinois: Fitzroy Dearborn Publishers, 2000), 40.

[36] R. Ernest Dupuy and Trevor N. Dupuy, *The Encyclopedia of Military History from 3500 B.C. to the Present*, 2nd ed. (Toronto, Canada: Harper and Row Publishers, Inc., 1986), 344.

[37] *Ibid.*, 344.

[38] WordiQ.com, "Auld Alliance," http://www.wordiq.com/definition/Auld_Alliance.html; Internet; accessed 26 March 2005.

[39] British Broadcasting Corporation, "The Auld Alliance 1295," http://www.bbc.co.uk/history/timelines/scotland/auld_all.shtml; Internet; accessed 26 March 2005.

with Highland forces with an operating or limited English language skill were trained to work together using English commands. Meanwhile, those Highland forces with only Gaelic language skills "…who fought very individualistic[ally] by nature, were used as his secret reserve."[41] By educating his forces to understand a common language base of commands prior to the engagement, Bruce had prepared the men to respond quickly to changes during the battle. Whether this decision was persuasive in winning the battle for Bruce is unknown; however, it does provide adequate evidence of the need for a common language or at the least common understanding of commands for fielded forces.

As to the intelligence during the medieval era, the use of spies was a common practice among nations to collect intelligence information on the enemy. "Spies generally operated under the guise of merchants or traders."[42] It was Philippe De Commynes in the 1470's who stated that "…messenger, spy and diplomat amount to the same thing."[43] Although diplomats of the time were advised not to conduct themselves as spies, most understood that "…the primary function of the post of resident ambassador was as political intelligence officer."[44] Regardless of the relationship between spying and diplomacy, anytime critical information was collected, it would then be passed to couriers, who in turn would

---

[40] R.M. Gunn, "The Bruce Bannockburn and Beyond," *AOL.Hometown* (2003); available from http://members.aol.com/skyelander/bruce1.html; Internet; accessed 3 April 2005.

[41] *Ibid.,* accessed 3 April 2005.

[42] R. Ernest Dupuy and Trevor N. Dupuy, *The Encyclopedia of Military History from 3500 B.C. to the Present*, 2nd ed., 343.

[43] Ian Arthurson,"Espionage and Intelligence from the War of the Roses to the Reformation," *Nottingham Medieval Studies*, Version 35 (1991) [article on-line]; available from http://www.deremilitari.org/RESOURCES/ARTICLES/nottinghammedievalstudies.htm; Internet; accessed 3 April 2005.

[44] *Ibid.,* accessed 3 April 2005.

notify the appropriate national authorities for use. "When battle was imminent

and lines of communication shortened intelligence was provided by footmen and

numerous scouts, scourers, prickers, fore riders, and harbingers."[45] However,

each piece of intelligence must be gauged carefully, as feints at this time could

play a vital role in shaping the outcome of battles. Once again, we can return to

the Battle of Bannockburn for a clear example of this.

> "While armies were locked in combat on the slope above the stream,
> the Scottish camp followers decided to pretend an attack through the woods
> against the English left flank. Blowing horns, waving banners, and simulating a
> large combat force, they approached the English left, which began to crumble.
> Edward himself decided to leave the battlefield, and his craven example was
> soon followed by most of his army. The Scottish pursued, slaughtering
> thousands of Englishmen trying to struggle back across the stream and the
> marsh."[46]

Had Edward received better intelligence from his troops fighting on the left flank,

he may have not departed so hastily or at so high a cost. Besides feints, one of the

most limiting factors of intelligence sharing for the Auld Alliance was the

extended line of communication necessary to cross in order to effectively pass

information to allies. Any communications between France and Scotland would

require longer lead times and the traversing of unfriendly open waters, inviting

the possibility of English interception.

Axis and Allies

By the early Twentieth century the art of alliances and coalitions had grown in

complexity across the globe. Although the assassination of the Archduke of Austria,

Franz Ferdinand in Sarajevo served as the impetus for the onset of World War I, "…the

---

[45] *Ibid.,* accessed 3 April 2005.

[46] R. Ernest Dupuy and Trevor N. Dupuy, *The Encyclopedia of Military History from 3500 B.C. to the Present*, 2nd ed., 366.

complex web of alliances and counterbalances that developed between the various European powers…"[47] played a critical role in the eruption of warfare between European states in 1914. The nature of the alliances allowed or forced members of both sides to join the campaign. For Austria-Hungary, "…Germany readily agreed, [and] even encouraged Austria-Hungary's warlike stance."[48] Western European and North American states were drawn into a conflict between Austro-Hungary and Serbia by a complex linkage of agreements starting with a Russo-Serb pact and ending with Britain's guarantee of Belgian neutrality.

Besides the growing complexity of alliances, the nature of warfare had transformed rapidly as well. The implementation of aerial balloons and small aircraft would rapidly advance over the course of the war. In fact, on 22 August 1914, a British pilot warned of an impending German attack on British forces and based on this intelligence, the British "…started a retreat toward Mons--destroying morale but saving the lives of 100,000 soldiers."[49] With both inproved gunnery and bombardment capabilities, aircraft would take center stage with air proponents around the world following the war. In the water, German U-boats or submarines provided unprecendented results threatening the very lifelines of Britain. Still, "…it was the

---

[47] Wikipedia, "World War I," http://en.wikipedia.org/wiki/World_War_I; Internet; accessed 5 February 2005.

[48] Michael Duffy, "The Causes of World War I," *FirstWorldWar.com*, Featured Article (27 March 2004) [article on-line]; available from http://www.firstworldwar.com/origins/causes.htm; accessed 20 March 2005.

[49] Pamela Feltus, "Aerial Reconnaissance in World War I," http://www.centennialofflight.gov/essay/Air_Power/WWI-reconnaissance/AP2.htm; Internet; accessed 22 March 2005.

decision to lift restrictions on submarine activity…"[50] that would ultimately bring the United States into the conflict.

World War I also became a proving ground for the wireless radio. Central Powers began utilizing Marconi's[51] wireless telegraphy as the primary means of communication to fielded forces. Allied forces equally used Marconi's technology to relay movement plans and coordinate strikes on the enemy trenches. In fact, "Reconnaissance aircraft that had enough power to carry wireless sets (they weighed 50kg) were able to communicate the position of enemy artillery."[52] This new communications capability would make aerial observation aircraft "…invaluable to the contending armies."[53] By the end of the war aircraft were conducting "…specialized functions-pursuit, observation, day bombardment, and longe-range night bombardment-that required distinctive attributes in the machines being used."[54] Unfortunately for the planes equipped with radios, "…the service was never satisfactory or reliable and had little influence on military operations."[55]

---

[50] Wikipedia, "World War I," http://en.wikipedia.org/wiki/World_War_I: Internet; accessed 5 February 2005.

[51] Gugliemo Marconi improved upon Heinrich Hertz's demonstration of radiation to include the building of a receiver and transmitter widely used to transmit vocal messages, for further information see Spartacus Schoolnet, "Wireless Communications," http://www.spartacus.schoolnet.co.uk/FWWwireless.htm; Internet; accessed 6 Feb 2005.

[52] *Ibid.,* accessed 6 Feb 2005.

[53] Bernard C. Nalty, *Winged Shield, Winged Sword: A history of the United States Air Force* (Washington, D.C.: U.S. Government Printing Office, 1997), 36.

[54] *Ibid.*, 37.

[55] Encyclopedia Britannica Online, "Military Communications: From World War I to 1940," http://nasaa-home.org/history/his5comms.htm; Internet; accessed 6 February 2005.

On the ground, divisional forces utilized a wide array of communications systems ranging from "…telephones, flags, and lanterns, and dispatch riders on motorcycles, bicycles, or horses."[56] By the early 20th century, the methods of communications may have changed; however, the overriding importance of interoperability during World War I remained. Senior military war planners would design campaigns from a safe distance and rely on field officers to exercise local command and control of forces. The fog and friction present at the beginning of a push forward many times would negate a majority of the possible communications techniques for transferring critical intelligence back to field commanders and headquarters personnel. "…If the infantry pierced the enemy line but could not signal their success to the generals, who were necessarily miles back, then vital decisions, such as committing reserves might be made either too late or not at all."[57] Telephones were used with the greatest degree of success. In fact, "The front, support and reserve lines were connected at frequent intervals by communication trenches, along which passed reliefs, rations, supplies of ammunition and telephone cables to battalion and battery H.Q.s."[58] By transferring information over the telephone system, headquarters personnel could then notify allies, establishing some degree of interoperability.

However, for smaller units, "…telephone communications was out of the question; since companies and platoons were too numerous to supply with wire and

---

[56] Nikolas Gardner, *Trial By Fire: Command and the British Expeditionary Force in 1914* (Westport, Connecticut: Praeger Publishers, 2003), 44.

[57] Tony Ashworth, *Trench Warfare 1914-1918: The Live and Let Live System* (New York, New York: Holmes& Meier Publishers, Inc., 1980), 50.

[58] *Ibid.*, 5.

moved too quickly and erratically to follow effectively with signal sections…"[59]

Therefore, many units relied on other means of communicating and the transfer of

information remained a single-nation focus until the information slowly weaved its way

back to the headquarters. However, the lack of sufficient communications plagued the

Axis nations as well. "At one end of the scale was Great Britain, with a small but highly

developed signal service; and at the other end stood Russia, with a signal service inferior

to that of the Union Army at the close of the American Civil War."[60] In one example, the

lack of adequate lines of communication by German forces "…caused a miscarriage of

the plan, a forced halt in the German advance, and the subsequent withdrawal north of the

Marne."[61]

For the Axis nations, language also played a central role confusing both political

and military operations. Directly following Franz Ferdinand's assassination, an

immediate and limited retaliation by Austria-Hungary against Serbia might have been

expected and potentially accepted by other European countries. However, the diversity

of the national population required a mobilization order to appear "…in some twenty

different languages - testimony to the tolerance but also to the impracticality of the

empire."[62] This language barrier would cause even greater strife in the greater Axis

alliance with Germany. "Germany and Austria-Hungary suffered from

---

[59] Bill Rawling, *Surviving Trench Warfare: Technology and the Canadian Corps, 1914-1918* (Toronto, Ontario: University of Toronto Press, 1992), 126.

[60] Encyclopedia Britannica Online, "Military Communications: From World War I to 1940," accessed 6 February 2005.

[61] *Ibid., accessed* 6 February 2005.

[62] Raffael Scheck, "Germany and Europe, 1871-1945," [book on-line]; available from http://www.colby.edu/personal/r/rmscheck; Internet; accessed 23 March 2005.

miscommunication regarding each army's intention."[63] Austria-Hungary expected

German support for the invasion of Serbia, whereas Germany expected Austria-Hungary

to provide forces to support the entire Eastern front of the war while Germany focused on

the West. This lack of effective multinational communication "…forced the Austro-

Hungarian army to split its troop concentrations in the south to meet the Russian

aggression in the north."[64]

On the allied front, although language problems were minimal, they were present

even among American forces. "During the First World War, the U.S. government drafted

into military service nearly half a million immigrants of forty-six different nationalities,

creating an army with over 18 percent of its soldiers born in foreign countries."[65] To

ensure soldiers would be able to understand commands on the battlefield, they were

required to attend "…three hours per day of English classes as part of their mandatory

military duties."[66]

"The first major demand during the twentieth century for improved U.S.

intelligence came during World War I."[67] With the use of aerial balloons, aircraft,

infantry and spies, allied forces were able to begin collecting critical information on the

enemy. Many times this information was only passed to national personnel, but in

several instances intelligence sharing did occur. In fact, at the battle of Amiens "one

---

[63] Wikipedia, "World War I," http://en.wikipedia.org/wiki/World_war_I: Internet; accessed 6 February 2005.

[64] *Ibid.,* accessed 6 February 2005.

[65] Nancy Gentile Ford, *Americans All! Foreign-born Soldiers in World War I* (College Station, Texas: Texas A&M University Press, 2001), 3.

[66] *Ibid.*, 107.

[67] Mark M. Lowenthal, *U.S. Intelligence: Evolution and Anatomy*, 2nd ed. (Westport, Connecticut: Praeger Publishers, 1992), 6.

report by the Australian Corps is of particular note, as indicating that the deficiencies among the enemy were not confined to their frontline troops."[68] This report was received by British leadership who in-turn capitalized off the information and planned an appropriate attack on the weak area. Aerial photographs proved the most useful intelligence to forces in WWI, as in the case of Sir Henry Rawlinson. By 1917, photographed aerial shots could be "…transposed onto up-to-date maps."[69] From there Rawlinson and his artillerymen could direct barrages with "precision on their German Counterparts."[70]

Operation Iraqi Freedom

In twenty-first century, the United States has struggled to find support for operations from traditional alliances and has turned to "Coalitions of the willing [that] can augment these permanent institutions."[71] The most recent example of this is the coalition established for Operation Iraqi Freedom.

In the months preceding the war, U.S. "…diplomats conducted frenzied negotitations to enlist allies and gain U.N. support."[72] However, the plan for Operation Iraqi Freedom met with heavy resistance from several North Atlantic Treaty Organization (NATO) countries and many United Nations representatives. Germany, France and Belgium resistance to the use of NATO forces "…frustrated a NATO-derived coalition

---

[68] Robin Prior and Trevor Wilson, *Command on the Western Front* (Cambridge, Massachusetts: Blackwell Publishers, 1992), 301.

[69] *Ibid.*, 295.

[70] *Ibid.*, 295.

[71] The White House, *The National Strategy of the United States of America* (Washington, D.C.: U.S. Government Printing Office, September 2002), vi.

[72] Marc Kusnetz, William M. Arkin, General Montgomery Meigs (Retired), and Neal Shapiro, *Operation Iraqi Freedom* (Kansas City, Missouri: Andrews McNeel Publishing, 2003), xii.

and left scars that may see the unraveling of the alliance as we know it."[73]   However,

after 12 years of U.N Security Council Resolution failures, the United States realizing

that no agreement could be forged from either NATO or the U.N. prior to the

engagement of force, boldly pursued a "Coalition of the Willing." This arrangement

included some traditional alliance partners of the United States, as well as, new coalition

partnerships with nations seeking greater political, economic or military ties with the U.S.

Regardless of the motivational factors of the various nations coupled together to form the

coalition, each nation determined it was within the nation's interest to politically and/or

militarily support the operation.

By examining Operation Iraqi Freedom, one can ascertain that knowledge-sharing

systems have not only begun to be considered, but they have created even greater

interoperability challenges among potential multinational partners. In a recent study

conducted by the European Institute, it concluded "that international coalition operations

have been significantly hampered in recent years by a perceived and real lack of

compatibility between military capabilities of the United States and those of Europe."[74]

This is not to say that traditional alliances, such as NATO, have not maintained minimal

standards for operations, just that the United States defense investments have resulted in

rapid growth in the information spectrum of operations.

The truth of the matter is several U.S. information systems capabilities have

surpassed their multinational partners and this disparity led to problems during the

conflict in Iraq. In fact, "Sharing information and the interoperability of information

---

[73] *Ibid.*, xii.

[74] Elizabeth G. Book, "Are Europeans willing to invest in interoperability?" *National Defense Magazine*, Volume 87, Iss. 589 (December 2002): 34.

systems were among the greatest challenges facing the coalition."[75] One prime example

of this occurred during the Operation Iraqi Freedom invasion in which a U.S. A-10 failed

to accurately identify two British reconnaissance Scimitar vehicles and conducted two

consecutive strafing runs. British forces present at the time stated that both vehicles had

clear coalition markings and on "…the back of one of the engineers' vehicles there was a

Union Jack."[76] If forces are unable to interoperate with U.S. systems, they may cause

gaps in command and control, situational awareness, and potential blue-on-blue

situations. Because the pilot had no indication from the Identify Friend or Foe (IFF)

indicators, he was cleared to engage the target. Several international or U.S. information

tools could have prevented this tragedy such as Identify Friend or Foe (IFF) or the

version available at the time of Joint Blue Force Tracking (JBFT); however,

interoperability issues had not been completely worked out at the time.

However, interoperability was not the only problem that plagued coalition

operations, intelligence problems at both the political and military levels equally caused

strife in coalition development and operations. Many alliance partners, such as France

and Germany, declined to participate. Whether one agrees that each nation was

threatened by the perceived Weapons of Mass Destruction (WMD) thought to be owned

by Iraq or not, each nation was forced to determine whether or not the coalition was in

their best interests based on the knowledge available to them at that time. According to a

Senate Committee report on the Central Intelligence Agency's intelligence information

---

[75] Squadron Leader Sophy Gardner, "Operation Iraqi Freedom: Coalition Operations," *Air & Space Power Journal,* Volume XVIII, No. 4 (Winter, 2004): 95.

[76] Gaurdian Unlimited, "Wounded British soldiers condemn US 'cowboy' pilot," http://www.guardian.co.uk/Iraq/Story/0%2C2763%2C926237%2C00.html; Internet; accessed 7 February 2005.

on Iraq, "…accused the intelligence community of 'group think,' 'poor management' and 'inadequate intelligence collection.'"[77] The intelligence data that the United States released to potential alliance and coalition partners was not adequate enough to convince specific countries of the threat to their national sovereignty. Following the invasion of Iraq, the Cambridge Endowment for International Peace published a report stating, "Iraq's [weapons of mass destruction] WMD programs represented a long-term threat that could not be ignored. They did not, however, pose an immediate threat to the United States, to the region, or to global security."[78] Therefore, whether by agenda or intelligence, several alliance members could soundly justify non-participation.

With respect to military operations, progress may continue, but nations' ability to share intelligence was a persistent challenge in Operation Iraqi Freedom. Although, "…the limited extent of the…coalition made information and intelligence sharing easier…the frustration came in translating the trust engendered at the highest levels into sensible information sharing at the lower level."[79] While the United Kingdom was granted access to the U.S. Secret network, other nations including Australia were initially relegated to using the new Combined Enterprise Regional Information Exchange System or CENTRIX. "CENTRIXS is now the premier network for coalition interoperability in support of military operations."[80] However, every time the British personnel needed to

---

[77] "Only America Unhappy with Iran," *American Foreign Press*, Volume 2, Issue 886 (February 2005) [article on-line]; available from http://www.thebangladeshtoday.com/archive/February/14-02-2005.htm; Internet; accessed 7 April 2005.

[78] Joseph Cirincione, Jessica T. Mathews, George Perkovich and Alexis Orton, *WMD in Iraq: Evidence and Implications* (Washington, D.C.: Cambridge Endowment for International Peace, 2004), 47.

[79] Squadron Leader Sophy Gardner, "Operation Iraqi Freedom: Coalition Operations," 95.

share information with other coalition partners besides the U.S., it required U.S. intervention to "…find the time…to decide on and implement the transfer of information."[81] Several of these problems could have been alleviated with the development and incorporation of multi-level security networks.

When one looks at the Iraqi Freedom coalition, again the issue of language becomes a barrier for effective operational execution. However, in this instance the problem manifested itself in two distinct ways. First, as seen in the other alliance examples, the traditional problem of coalition partners speaking in various languages or experiencing terminology definition problems. NATO attempted to resolve this by establishing two official languages, English and French, and by issuing standard terminology descriptions in both languages for use with other NATO members. The UN has equally established six official languages and a database of standard terms from which to deal with its members. However, unless non-traditional coalition partners linguistically trained their forces to interact with the U.S., language difficulties would remain persistent.

The second challenge in Iraq dealt with interaction of the indigenous people of Iraq. As Gunner J.L. Eby states it "Civilians died because of our failure to plan for methods of stopping traffic from entering our zones of operations."[82] The inability of Marines to communicate adequately either through verbal or non-verbal means led

---

[80] Jill L. Boardman, "Combined Enterprise Regional Information Exchange System (CENTRIXS); Supporting Coalition Warfare World-wide," http://www.dodccrp.org/events/2004/ICCRTS_Denmark/CD/papers/003.pdf; Internet; accessed 7 April 2005.

[81] Squadron Leader Sophy Gardner, "Operation Iraqi Freedom: Coalition Operations," 96.

[82] Gunner J.L. Eby, "I Told You So," *2nd Battalion, 5th Marines Website* [article on-line]; available from http://www.2ndbn5thmar.com/oif/told%20you%20so.htm; Internet; accessed 7 April 2005.

innocent civilians to act in unpredictable ways as Marines "resorted to firing a warning burst at the approaching traffic."[83] As Gunner Eby in his report points out a simple item such as "…having 'stop' signs in the language of the country we're attacking,"[84] would assist with public understanding of the intentions of forces.

Based on each of the historical snapshots, whether between allies or coalition partners, communication has and will continue to play a critical role in the conduct of military operations. Issues relating to interoperability, language barriers and intelligence have long plagued the multinational environment and yet these areas can significantly contribute to the success of an operation. Nations that fail to adequately share critical knowledge with multinational partners risk potential friendly fire incidents and the underutilization of allied forces.

---

[83] *Ibid.,* accessed 7 April 2005.

[84] *Ibid.,* accessed 7 April 2005.

SECTION 3

ENHANCING DECISION-MAKING: BENEFITS

AND CHALLENGES TO KNOWLEDGE SHARING

> The basic challenge in multinational operations is the effective integration and employment of all assets provided toward the achievement of a common objective.
> - Joint Publication 3-16

So what are the advantages of sharing knowledge with other countries? To begin, one should start with the benefits it can create at the initial formulation of multinational support for an operation. As mentioned several times throughout the document, nations will tend to join alliances or coalitions only if it appears to serve their own interest. "Since human nature has not changed, regional conflicts over territory, religion, politics, and economics, such as those that prompted previous military operations, will continue to be widespread."[85] Based on this fact, it will be incumbent upon nations to provide, reliable and accurate knowledge to persuasive enough to compel nations to combine efforts in a multinational operation. "It is safe to assume that most allies seek both political and military advantages from any alliances."[86] Then depending on each nation's interests coupled with the influence of its political leadership a determination for joining will be made. However, if politicians are not armed with sufficient evidence that a threat

---

[85] Secretary of the Army, *Field Manual 100-8: The Army in Multinational Operations*, (Washington, D.C.: U.S. Government Printing Office, February 1999), vi.

[86] Robert L. Rothstein, *Alliances and Small Powers*, 50.

exists or that somehow their national interests are at risk, politicians may be unable to

garner constituency support. This equally applies to international political institutions

such as NATO and the UN. "The overall effectiveness of U.N. decisions will depend on

the quality of the information available."[87] By utilizing knowledge sharing systems,

nations can broaden their persuasiveness to seek multinational partners by providing

reliable and accurate knowledge to UN leadership as well. However, this is not to say

that nations such as the U.S. should share all knowledge with international organizations.

"Depending on the situation and what U.S. interests are at stake, we will determine what

sensitive information, if any, to share with the U.N."[88]

Once multinational support is established, it then becomes critical to develop

linkages in order to share knowledge with multinational militaries participating in the

operation. As noted in the caption opening this section, "The basic challenge in

multinational operations is the effective integration and employment of all assets

provided toward the achievement of a common objective."[89] If all assets are to focus on

satisfactorily reaching a common objective, they must therefore have a common

understanding of the environment in which they are operating. "Members of

multinational operations need to share intelligence if they are all to react to the same

threat environment in an acceptable way (but not necessarily an identical way)."[90]

---

[87] Commander Charles A. Williams, "Intelligence Support to U.N. Peacekeeping Operations" (Washington, D.C.: National Defense University Industrial College of the Armed Forces Paper, 1993), 7.

[88] *Ibid.,* 21.

[89] Joint Chiefs of Staff, *Joint Publication 3-16: Joint Doctrine for Multinational Operations*, III-1.

[90] Eric S. Miller, "Interoperability of Rules of Engagement in Multinational Maritime Operations," 33.

Advantages in knowledge sharing are already evident in more traditional alliances such as the America, Britian, Canada, and Australia (ABCA) program. "In Iraq, ABCA members were interoperable primarily because of shared procedural measures, the use of liaison officers and doctrinal compatibility."[91] The next step would be to expand such capabilities to smaller, more non-traditional multinational partners to create opportunities for emerging nations to participate effectively in modern multinational operations. By effectively extending interoperability to emerging nations, the nations will ultimately create linkages from which to pass critical knowledge sharing specific to the needs of a supporting nation.

If implemented properly knowledge-based systems can ultimately lead to a shorter decision cycle for operational and fielded commanders, thereby improving the command and control of forces. Organizations such as NATO have equally recognized the need for integrated command and control systems to aid forces. "To ensure military effectiveness in future operations, which are likely to be multinational and quite often involve brigade-size units, NATO will need a joint and combined command-and-control capability."[92] So what are the factors in the decision cycle knowledge sharing can affect? A decision cycle is the time an "…entity takes to make a decision based upon the scope of its responsibilities, its current physical and physiological state, and the quantity and

---

[91] Lieutenant Colonel Robert L. Mcginnis (Retired), "Keeping our Best Army Coalition Relevant by Transforming Together," *Army Magazine* (September 2003) [article on-line]; available from http://www.ausa.org/www/armymag.nsf/0/003C39EC1847B53185256D860061211F?OpenDocument; Internet; accessed 20 March 2005.

[92] Richard Sokolsky, Stuart Johnson, and F. Stephen Larrabee, *Improving Allied Military Contributions*, 43.

quality of information it receives."[93] By implementing knowledge sharing, the system

can draw out pertinent information necessary for a commander to review before making a

decision, thereby enhancing the "quality and quantity" and reducing this factor as a

stressor in the decision cycle. However, the system must remain flexible to provide

additional information or knowledge as requested by commanders as new developments

in the campaign evolve.

Once a knowledge sharing system is in place, forces can then focus "…personal

and professional relationships with counterparts in other nations."[94] This statement

captures the requirement for liaison officers, to aid multinational leaders interpret the

shared knowledge. Or as Scales puts it, "…geostrategic scouts that have the requisite

language, cultural, historical, and regional geopolitical knowledge to assist [alliance or]

coalition commanders when they move into certain regions of the world."[95] These

geostrategic scouts can then create benefits for all nations involved. "By coordinating

issues on deployment, courses of action, rules of engagement, communications,

procedures, doctrine, and capabilities, tasks can be ultimately assigned that take into

account national sensitivities such as pride, honour and prestige."[96]

---

[93] Command, Control, Communications Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Modeling and Simulation Branch, *Integrated Decision Systems: Command and Control of the Future* (Rome New York: Rome, Laboratories, April 2004) [article on-line]; available from http://www.afrlhorizons.com/Briefs/Apr04/IF0315.html; Internet; accessed 20 March 2005.

[94] Robert H. Scales, Jr., "Trust, not technology, Sustains Coalitions," *Parameters*, Volume XVIII, no. 4 (Winter 1998), 5.

[95] Colonel C.J.R. Davis, "Command and Control in Coalition Operations" (Toronto: Cnanadian Forces College Advanced Military Studies Course Paper, 2000), 17.

[96] *Ibid.,* 16.

One of the most devastating events in conflict that potentially influences multinational operations is fratricide, commonly referred to as blue-on-blue accidents. "Fratricide was the second greatest cause of coalition casualties during the [Operation Desert Storm] Gulf War."[97] The ability to clearly differentiate between friendly or adversarial forces is critical to successful multinational operations. In Operation Desert Storm the "…inability to track identification, friend or foe (IFF) in the confused, rapidly developing scenario of the Gulf War led to blue-on- blue engagements."[98] Therefore, knowledge sharing with respect to the tracking and delineation of ALL multinational forces should be among the Joint Forces Commander's top priorities. If a coalition member suffers heavy fratricide casualties, they are less likely to continue to operate within the threat environment. Hence, any blue force tracking capability needs to provide expandability to incorporate multinational forces. Keeping in mind system information integrity, multinational forces should be equipped with portable devices that allow accurate and standardized tracking. Although initial implementation may come at a cost, the benefit of a single integrated system reduces the redundancy of specific national systems and eliminates blue-on-blue issues associated with incompatibility. "Minimizing redundant requirements…results in enhanced interoperability and synergy as each ally provides some critical function to achieve the desired collective effects."[99]

By increasing knowledge sharing between nations in an operation, each nation can draw upon a greater intelligence base for required information to support the

---

[97] Captain Daniel T. Keuhlan (USN), *The Common Operating Picture in Joint Vision 2020: A Less Layered Cake* (Joint Forces Staff College Research Paper, May 2002), 6.

[98] *Ibid.*, 6.

[99] Colonel William H. Parry, III, "Multinational Operations and the National Security Strategy: The Modern Melian Dialogue," 26.

operation. As Jeffrey Richelson points out, by creating intelligence sharing relationships

"A nation may acquire useful intelligence that it is unable, for a variety of reasons, to

acquire otherwise."[100] As mentioned earlier nations may enter into multinational

operations with nations who have very limited resources, which is to say limited

intelligence assets as well. It is therefore necessary for nations with greater intelligence

> Historically, the problems of interoperability have been solved — when they have been solved at all — primarily through trial and error during actual conduct of operations over an extended period of time.
> - Joint Publication 3-16

capabilities to provide limited access to other member nations to ensure continuity of

effort. "With the right information, our warfighters and decision makers can more

readily identify threats, locate targets, and make critical decisions about the use of our

armed forces or intelligence assets."[101] In establishing intelligence sharing, nations can

then turn to the business of influencing "…the behavior of other nations – towards itself

or towards third nations…"[102] in a concerted fashion.

 However, the sharing of knowledge, let alone intelligence, does not come without

significant challenges. The first major challenge deals with interoperability. Again, one

can easily understand there will be disparities in information systems technology between

multinational member states. To overcome this disparity, the argument leans again

toward a solution set in which nation, such as the U.S., with a greater degree of

---

[100] Jeffrey T. Richelson, "The Calculus of Intelligence Cooperation," *International Journal of Intelligence and Counterintelligence*, Volume 4, no. 3 (Fall 1990), 311.

[101] Intelligence Community Metadata Working Group (IC MWG), *Metadata and XML: Defining a New Intelligence Paradigm* (April 2003) [article on-line]; available from https://www.xml.saic.com/icml/xnotes/MetadataXML/MetadataXML.html; Internet; accessed 13 April 2005.

[102] Jeffrey T. Richelson, "The Calculus of Intelligence Cooperation," 311.

knowledge sharing capability, extend this capability to other nations. The argument then

turns to "the how" to provide limited access to secure national systems. Multilevel

Security (MLS) systems include those which contain "…information with different

sensitivities that simultaneously permits access by users with different security clearances

and needs-to-know, but prevents users from obtaining access to information for which

they lack authorization."[103] Therefore, in order to effectively share knowledge, the

system must not only provide other nations with access to an interoperable system, but

must control the level of access and influence individual users may have over the system.

For if the system allows to great of access and influence "…allies can exploit cooperative

arrangements to conduct espionage against their partners."[104] Therefore the system must

be able to prevent exploitation of critical information by allies, whether by design or

accident, in an adversarial way. The idea behind MLS here is to "…seek to prevent a

hostile piece of software from leaking high-level (e.g., secret) information to low-level

(e.g., uncleared) users."[105]

Knowledge sharing systems must not only take into account differences in host

national personnel access, but also the differences in access required for both traditional

allies and emerging coalition partners. For example, when dealing with host national

personnel, "…if an intelligence report exceeds the classification level of a unit's

[103] First Lieutenant Michael C. Cerone, "Multilevel Network Security," *Hill Air Force Base Crosstalk* (September 1995) [article on-line]; available from http://www.stsc.hill.af.mil/crosstalk/1995/09/Multilev.asp; Internet; accessed 20 March 2005.

[104] James J. Wirtz, "Constraints on Intelligence Collaboration: The Domestic Dimension," *International Journal of Intelligence and Counterintelligence*, Volume 6 no.1 (Spring 1993), 89.

[105] *Realizing the Potential of C4I: Fundamental Challenges* (Commission on Physical Sciences, Mathematics, and Applications, National Research Council Committee to Review DOD C4I Plans and Programs, 1999) [book on-line]; available from http://books.nap.edu/html/C4I/index.html; Internet; accessed 20 March 2005.

communication system or operating level the report should be sanitized after coordinating release, and then transmitted to the unit for effective use."[106] This requirement to sanitize knowledge before it is released to lower levels is central to the argument for MLS. Currently U.S. agencies "…rely on processes for 'sanitizing' classified information so that it can be shared with other agencies…but the sanitized version is often still classified."[107] This inability to adequately sanitize knowledge for use at lower levels leads to the inability to release knowledge to lower levels. Likewise, in the multinational arena, "…a multilevel security system does not currently exist that can easily facilitate sanitization and dissemination of intelligence to U.S. and allied and/or coalition operational commanders."[108] Therefore to reduce the possibility of inadvertent release of classified information while ensuring knowledge transfer, automated system processes commonly called screening tools are a must! "Screening tools can automatically alert disseminators when potentially sensitive information is about to be transmitted, or when information may be about to be sent to parties that lack the requisite permission to receive it."[109] The system must provide the capability to strip off classified host nation only information and disseminate the required knowledge to the respective multinational commander.

---

[106] Secretary of the Army, *Field Manual 34-2: Collection Management and Synchronization Planning* (Washington, D.C.: U.S. Government Printing Office, 1994), 3-21.

[107] Bill Cromwell, *Too Many Secrets: Overclassification as a Barrier to Critical Information Sharing* (Testimony Before the Subcommittee on National Security, Emerging Threats, and International Relations House Committee on Government Reform, August 2004), 2.

[108] Joint Chiefs of Staff, *Joint Publication 2-01: Joint and National Intelligence Support to Military Operations* (Washington, D.C.: U.S. Government Printing Office, October 2004), V-13.

[109] *Ibid.,* 3.

U.S. military commanders are charged with operating "…alongside alliance or coalition forces, integrating their capabilities and capitalizing on their strengths, to promote regional stability throughout the world,"[110] and therefore must establish how selected information will be transmitted to multinational users? For the United States Army, "Knowledge-based C4I systems will foster the ability to *push* designated information to the user while simultaneously permitting the user to *pull* additional information from the digital environment as needed."[111] By using push technology, the command and control system can automatically, cleanse knowledge of restricted data and "push" the critical information down to the awaiting commander. This would constitute a majority of the information emerging allies would have access to for the duration of the operation. Equally, depending upon the trust relationships built between nations, the ability to "pull" or request data outside the normal push could be granted.

Since political motivations of potential multinational partners will always play a role in the feasibility and efficiency of a multinational operation, it is equally important to ensure effective knowledge sharing systems are integrated at the strategic/political level. "As long as the coalition members perceive their membership as advancing their individual national interests, then the coalition can remain intact."[112] If specific national objectives or interests become divergent, then the future of the coalition may be jeopardized. To this end, anytime a nation begins planning for multinational operations,

---

[110] Joint Chiefs of Staff, *Joint Publication 3-16: Joint Doctrine for Multinational Operations*, I-3.

[111] Secretary of the Army, *Army Digitization Master Plan '96* (Washington, D.C.: U.S. Government Priting Office, 1996) [article on-line]; available from http://www.globalsecurity.org/military/library/report/1996/army_digit_m-plan96.htm; Internet; accessed 10 April 2005.

[112] Joint Chiefs of Staff, *Joint Publication 3-0: Doctrine for Joint Operations* (Washington, D.C.: U.S. Government Printing Office, September 2001), VI-1.

it is imperative that they develop MLS-like interconnectivity to provide the appropriate level of situational awareness to political leadership. "Situational awareness through digital technology will be the enabling technology for maintaining public support for the military, as well as keeping the political leadership from embarrassment."[113] However, this is not to say that political leadership should be provided the ability to scroll down into the system to gain granularity at the tactical level. If granted that level of access, "the pressure to micro-manage, to ask questions, and to second guess field commander's decisions will be very high."[114] Therefore, knowledge sharing can provide benefits at the political level, but the degree of knowledge must still provide military leadership the latitude to perform operations.

The last major area of concern deals with the misinterpretation of knowledge information. When networks are opened to users working under multinational conditions, the threat of erroneous interpretation can be exacerbated by different language standards and ineffective use of accurate terminology. "Multinational forces may have differences in [Command, Control, Communications and Computers] C4 systems, languages, terminology, doctrine, and operating standards that can cause confusion."[115] The language barrier and misinterpretation of terminology alone can lead to confused execution of operations.

---

[113] Lieutenant Colonel Steven J. Fox, "Unintended Consequences of Joint digitization," *Sun Tzu Art of War in Information Warfare* (National Defense University Institute for International Studies, 2002) [chapter on-line]; available from http://www.ndu.edu/inss/siws/cont.html; Internet; accessed 8 April 2005.

[114] *Ibid.,* accessed 8 April 2005.

[115] Joint Chiefs of Staff, *Joint Publication 6-0: Doctrine for Command, Control, Communications, and Computers (C4) System Support in Joint Operations* (Washington, D.C.: U.S. Government Printing Office, May 1995), II-9.

To mitigate some of the problems associated with multinational miscommunication, joint forces commanders could attempt to utilize NATO and the UN established standard lists of terminology to promote international understanding. NATO has issued Allied Administrative Publication (AAP-6) that serves "…to standardize terminology throughout NATO, thereby promoting mutual understanding."[116] The UN has equally taken a proactive approach to attempt to bring mutual understanding to international terminology. Currently the UN utilizes the United Nations Multilingual Terminology (UNTERM) Database to track over 70,000 terms and their meanings in all six of the UN international languages.[117]

However, due to the large volume of terms and the risks associated with release of mission critical data, the requirement to develop a system capable of passing knowledge to multinational partners is critical to operational success. "To be successful operationally, a clear understanding of the national and military strategic goals and objectives is required."[118] Therefore, multinational representatives and liaison officers should be involved as early as possible in the planning process as a "…source of both formal and informal information exchange."[119] By involving multinational partners early in the process, communications and intelligence personnel can work together to formulate the appropriate operational objectives, training requirements, and system accessibility

---

[116] North Atlantic Treaty Organization (NATO), *NATO Glossary of Terms* (Brussels, Belgium: NATO Standardization Agency), VII.

[117] United Nations, UNTERM database, http://unterm.un.org/; Internet; accessed 19 March 2005.

[118] Col C.J.R. Davis, "Command and Control in Coalition Operations" (Toronto: Cnanadian Forces College Advanced Military Studies Course Paper, 2000), 5.

[119] Joint Chiefs of Staff, *Joint Publication 6-0: Doctrine for Command, Control, Communications, and Computers (C4) System Support in Joint Operations,* II-10.

required to ensure success. Member nations must understand not only how to interface

knowledge systems, but also understand the associated system security requirements.

How better to ensure knowledge receipt by multinational members than to co-

locate key personnel within each national command center. By providing liaison officers

well versed in both communications and intelligence, the lead nation can ensure that

effective dissemination of intelligence and knowledge is accomplished. One traditional

methods of breaching the language barrier is the use of "…sand tables, as a tool to

overcome language deficiencies when describing operational requirements."[120] This

approach may work well in an operation in which time is not a critical factor, but in

modern warfare, this approach can become time-consuming to the decision-cycle and

provide adversaries with potential opportunities to seize the initiative.

In the case of the United States, to become a force ready to deploy and provide

interoperability to emerging nations, U.S. armed forces will need to expand the status quo

for training bilingual officers.

> "U.S. military operations in Afghanistan and Iraq 'reinforce the
> reality that the Department of Defense needs a significantly improved
> organic capability in emerging languages and dialects, a greater
> competence and regional area skills in those languages and dialects, and a
> surge capability to rapidly expand its language capabilities on short
> notice'…"[121]

However, the 2004 Defense Language Transformation Roadmap points out that "A

generally proficient language professional is not a professional translator, interpreter,

---

[120] American-British-Canadian-Australian (ABCA) Program, *ABCA Coalition Operations Handbook* (Washington, D.C.: U.S. Government Printing Office, November 2001), 1-13.

[121] Jason Sherman, "Wolfowitz Approves Plan to Improve DoD's Foreign Language Skills," (U.S. Air Force Aim Points Inside the Pentagon Paper, March 2005) [article on-line]; available from http://aimpoints.hq.af.mil/display.cfm?id=1768; Internet; accessed 3 April 2005.

strategic debriefer, tactical interrogator, or cryptologic language analyst."[122] Therefore, a reasonable deduction can be made that both communications and intelligence personnel should be targeted for bilingual training to create liaison officers both proficient in the language and culture of the nation to be supported and proficient in understanding the communications and intelligence sharing requirements necessary to support the nation assigned. Once personnel are trained on a regional language, periodic assignments to regional locations aid in the understanding of both national military operations and the societal culture.

It is apparent nations will continue to pursue alliances and coalitions that act in their best interests and contain some commonality of objectives. However, a nation's ability to interoperate with others will create advantages over other forces that are only tied to a campaign by a common cause. A common understanding and knowledge base create singularity of action and increased situational awareness to all multinational forces. The ability to provide commanders with the knowledge necessary to plan and execute specific portions of an operation is critical to orchestrating modern warfare. Equally, the ability of these commanders to make decision in a more concise and expeditious fashion will shorten the decision cycle and provide swifter results in meeting mission objectives. Although there are several major challenges to overcome in dealing with knowledge sharing, by bringing multinational partners and liaison personnel into the operational planning process early on, combatant commanders can establish standards of language and procedure for use in the coalition environment. Equally, by establishing a sound rapport prior to hostilities, the lead nation can begin to verify clearance levels of the

---

[122] Department of Defense, *Defense Language Transformation Roadmap* (Washington, D.C.: U.S. Government Printing Office, June 2004), 25.

multinational workforce and ensure the right personnel have access to the right information at the right time. Limited access to multinational knowledge is critical for multinational partners to effectively plan and execute their respective portions of the operation. Last, by growing the number of language-qualified liaison personnel, lead nations can ensure effective knowledge sharing and interpretation of the intent of the knowledge is adequately transferred to other national forces. Therefore, again one finds that multinational interoperability, releasability of intelligence data, and the ability to linguistically aid in the interpretation and transfer of knowledge can add to the effectiveness of the operation.

SECTION 4

KNOWLEDGE-SHARING PROCESS

In accordance with the U.S. *Joint Vision 2020,* "The joint force must be able to take advantage of superior information converted to superior knowledge to achieve decision superiority."[123] The statement above captures the essence of this section, the knowledge sharing process. As with land-, sea-, air- and space-based operations, military leaders continue to seek new ways to effectively incorporate information strategies to achieve dominance over the enemy. The overall ability "…of US forces, operating unilaterally or in combination with multinational and interagency partners, to defeat any adversary and control any situation across the full range of military operations is known as full spectrum dominance."[124] Joint Vision 2020 outlines four pillars critical to achieving full spectrum dominance: Dominant Maneuver, Precision Engagement, Focused Logistics and Full Dimensional Protection. However, due to the steady increase of information technologies, technology dominance and information superiority have become key enabler to successfully meet all four of the pillars and effectively reach full spectrum dominance. Information superiority can only be achieved by mastering "…the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." To successfully develop

---

[123] Joint Chiefs of Staff, *Joint Vision 2020* (Washington, D.C.: U.S. Government Printing Office, December 2000), 8.

[124] *Ibid.*, 6.

systems and infrastructure to meet present and future full spectrum dominance requirements it is critical to outline the basic knowledge sharing process elements. Keeping in mind, "Intelligence sharing and interoperability are essential for responsiveness and dominance on the battlefield,"[125] this section will review the knowledge sharing process from collection to review by users for decision-making. Figure 4-1 provides a notional knowledge sharing process from which we can then delineate where various components and/or personnel action is then required to ultimately get knowledge to aid users in decision-making.
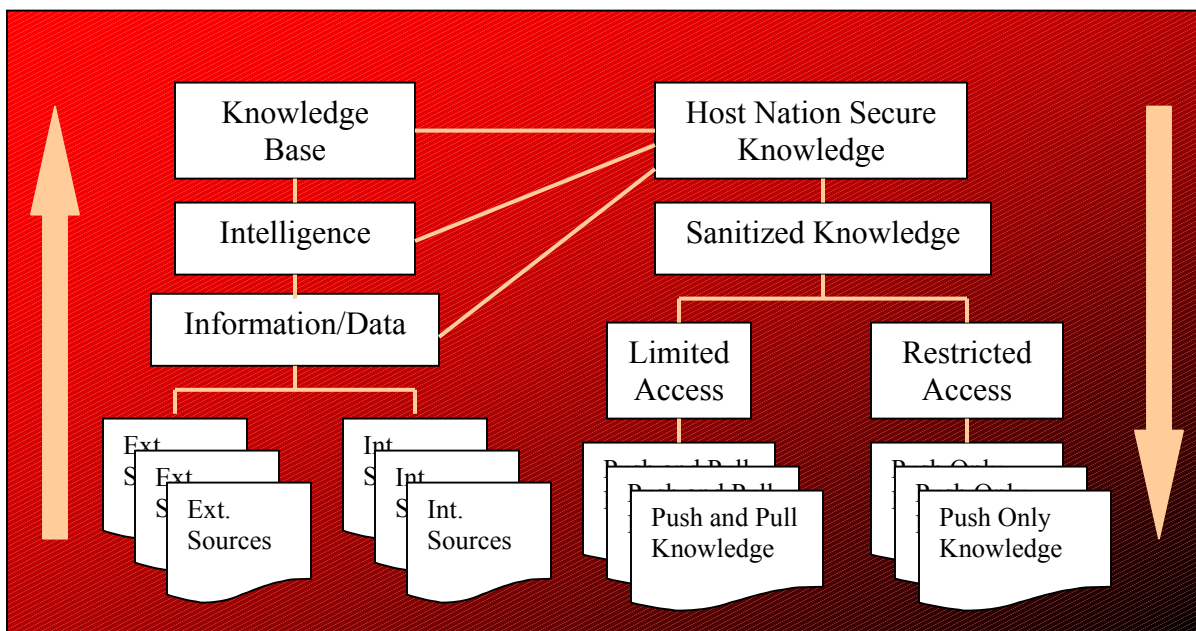
Figure 4-1: Knowledge Sharing Process

The first step in the process involves intelligences sources, sometimes referred to as sensors. Perhaps the most critical sensor is human intelligence or HUMINT. "From the covert agent, [Prisoner of War] POW, defector, to the overt military 'reconnoitire', it

---

[125] Major Michele H. Bredenkamp, "How Can the U.S. Army Overcome Intelligence Sharing Challenges Between Conventional and Special Operations Forces?" (United States Army Command and General Staff College School of Advanced Military Studies, 2002-2003), 7.

has been the human being who has been the most prolific source of intelligence before the advent of writing and the invention of the pictograph."[126] Although some HUMINT sources may become unreliable, it is understood that HUMINT must come from the most reliable sources possible. "Information coming from a trusted, competent, and respected source is more likely to be believed than rumor."[127] Much of what is collected by HUMINT sources is open source information. "The information is relatively cheap to obtain and makes up the greatest volume of information accessible to an intelligence collector."[128] The type and granularity of the information collected by HUMINT sources should determine the degree of sharing required amongst multinational partners.

Another source for intelligence data is the interception of communication information known as Signals Intelligence (SIGINT). "Interestingly, as more and more countries develop the ability to intercept signals and communication, they are also developing the ability to protect their transmissions from their adversaries."[129] SIGINT can be further broken down into three sub-categories: Communications, Telemetry and electromagnetic radiation intelligences or COMINT, TELINT, and ELINT respectively. COMINT is the oldest of the three and was used extensively during World War II. "German and Japanese communications were intercepted and decrypted, and vast amounts of accurate and timely information were made available to British and American

---

[126] Bhashyam Kasturi, "Military Intelligence in India: An Analysis" (1995) [article on-line]; available from http://www.bharat-rakshak.com/LANCER/idr00001.htm; Internet; accessed 2 April 2005.

[127] Steven Johnson, "Military Public Relations in the Americas: Learning to Promote the Flow" (Center for Hemispheric Defense Studies Research and Education in Defense and Security Studies Paper, May 2001), 8.

[128] National Security Agency, *Operations Security: Intelligence Threat Handbook* (Greenbelt, Maryland: The Interagency Support Staff, May 1996), Section 6.

[129] Arthur S. Hulnick, *Fixing the Spy Machine: Preparing American Intelligence for the Twenty-First Century* (Westport Connecticut: Praeger Publishers, 1999), 23.

political and military leaders."[130] TELINT is the "…interception, processing, and

analysis of foreign telemetry."[131] In other words, it's the collection of flying platform to

ground station data to gain insight to the parameters and potential capabilities of the

system. In cases such as missiles, "if the analysis is done fast enough, it might even

identify the location of the intended target."[132] ELINT is the last sub-category of

SIGINT, but can provide some of the most crucial data. "Knowledge of the electronic

order of battle (EOB) of the enemy is essential for planning offensive action against him

in order that concentrations of firepower may be avoided or destroyed as required."[133]

Military forces to collect and analyze intelligence on enemy electronic emitter systems

use ELINT. "By intercepting a radar signal, for example one can determine various

operating characteristics of the radar, such as its beam width and its maximum

operational range." [134] This intelligence is critical to the identification of radar coverage

and locations in which aircraft and missile assets might be vulnerable. Therefore, the

sharing of ELINT, or for that matter much of the theater SIGINT knowledge is critical to

successfully integrating the use of multinational assets into a campaign.

The third type of sensor data that might be collected involves photography

(PHOTINT) or better known as imagery intelligence (IMINT). "The most serious threat

---

[130] Abram N. Shulsky and Gary J. Schmitt, *Silent Warfare: Understanding the World of Intelligence*, 3rd ed. (Washington, D.C.: Brassey's Inc., 2002), 27-28.

[131] *Ibid.,* 27.

[132] Colonel George E. Daniels, "An Approach to Reconnaissance Doctrine," *Air University Review*, March-April 1982 (Air University Air War College Paper, 1982) [paper on-line]; available from http://www.airpower.maxwell.af.mil/airchronicles/aureview/1982/mar-apr/daniels.html; Internet; accessed 13 April 2005.

[133] *Ibid.,* accessed 13 April 2005.

[134] Abram N. Shulsky and Gary J. Schmitt, *Silent Warfare: Understanding the World of Intelligence*, 31.

from hostile IMINT resources at the strategic level stems from photoreconnaissance

satellites. At the tactical or field combat level, airborne collection possesses the greatest

IMINT threat."[135] Due to the current minimal threats to space assets, one can assume

that satellites might be the most significant asset overall. "Because there is little delay in

transmitting that data electronically from space to a ground station, imagery taken of a

target can be reproduced on earth virtually in 'real time' – that is, with negligible

delay."[136] However, since moving a satellite to the right place at the right time can

become a very expensive proposition, it is reasonable to assume that in the near term

Unmanned Aerial Vehicles (UAVs) and other airborne platforms will continue to provide

the greatest over-the-hill imagery to forces engaged in theater operations. This

perspective can be traced back to that of the air techniques used over World War I. As

Brigadier General Billy Mitchell, one of the biggest proponents for airpower at the time

stated, "one flight over the lines gave me a much clearer impression of how armies were

laid out than any amount of traveling around on the ground."[137] Regardless of whether

imagery is sourced through air or space means, the real issue then becomes one of

national classification. When operating internationally, "…classification of national

imagery must provide the required access to allies while continuing to protect

---

[135] United States, Secretary of the Army, "Army Regulation 530-1 OPSEC, Appendix D: The Hostile Intelligence Threat" (Washington D.C., 1985) [regulation on-line]; available from http://www.fas.org/irp/doddir/army/ar530-1d.htm; Internet; accessed 5 April 2005.

[136] Abram N. Shulsky and Gary J. Schmitt, *Silent Warfare: Understanding the World of Intelligence*, 22.

[137] Brigadier General William Mitchell, *Memoirs of World War I: "From Start to Finish of Our Greatest War"* (New York, New York: Random House, 1960), 59.

collection/processing capabilities."[138] This statement can easily be extended to include all multinational forces, in which, IMINT data is not only critical to the lead nation's campaign planning purposes, but also to the extensions of the multinational membership.

The last area of intelligence collection deals with the nuclear, biological, and chemical threat to multinational forces. Measurement and Signatures Intelligence (MASINT) "…include seismometers, which measure the shock waves associated with underground nuclear tests; devices to detect radioactivity associated with nuclear materials or the fallout of above-ground nuclear tests…to detect submarines under the oceans surface."[139] The idea behind MASINT is to collect and analyze many technical parameters of enemy systems. "MASINT can provide specific weapon system identifications, chemical compositions and material content and a potential adversary's ability to employ these weapons."[140] By understanding the capabilities of an adversary, one can begin to effectively offset or negate these capabilities in the development of the campaign plan. Therefore, again it is critical for a multinational knowledge system to be able to accept and provide MASINT information to multinational forces, while still protecting the means in which the data may be collected.

The second element in the Knowledge sharing process pertains to the information or data itself that is collected by various sources. "Information is raw data from any

---

[138] *The Intelligence Community of the 21st Century*, One Hundred Fourth Congress House of Representatives Staff Study, (June 1996) [study on-line]; available from http://www.au.af.mil/au/awc/awcgate/congress/ic21/ic21_toc.html; Internet; accessed 2 April 2005.

[139] Abram N. Shulsky and Gary J. Schmitt, *Silent Warfare: Understanding the World of Intelligence*, 31-32.

[140] *The Intelligence Community of the 21st Century*, accessed 2 April 2005.

source, data that may be fragmentary, contradictory, unreliable, ambiguous, deceptive, or

wrong."[141] With such a large variety and volume of data, the challenge then

becomes"…the effort by the intelligence community to process data into information that

can be disseminated to the customer in a useful form."[142] Much of the information

initially introduced to a knowledge system is considered raw intelligence data. This raw

information is then generally provided with a metadata "tag." "With the assistance of

metadata markup standards, intelligence system users can assure that information is

precisely recalled, repeatably accessible, accurate and available for reuse many times."[143]

By tagging raw information or data, it can then be stored into databases and retrieved as

required to support user requests. Currently, "the lack of available linguists for these data

increases the pressure for machine translation—especially because the material cannot be

tagged for archiving until it is translated."[144] Therefore, as raw data flows in, it will

require translation or the system will need to translate and tag information and generate

"…an abstract that summarizes the content of the item and metadata with a description of

the source, time, reliability-confidence, and relationship to other items."[145] Therefore

---

[141] United States, "A Brief History of Basic Intelligence and The World Factbook," *Central Intelligence Agency: The World Factbook* (December 2004) [article on-line]; available from http://www.odci.gov/cia/publications/factbook/docs/history.html; Internet; accessed 14 April 2005.

[142] Robert K. Ackerman, "Advanced Surveillance Spawns New Challenges," *Signal Magazine* (March 2004) [article on-line]; available from http://www.afcea.org/signal/articles/anmviewer.asp?a=28&z=10; Internet; accessed 16 April 2005.

[143] Wilson P. Dizard III, "Feds Expect XML to Ease Info Exchanges," *Government Computer Weekly*, Volume 21, No. 25 (August 2002) [article on-line]; available from http://www.gcn.com/21_25/news/19780-1.html; Internet; accessed 31 March 2005.

[144] Robert K. Ackerman, "Document Exploitation Increases in Importance," *Signal Magazine* (August 2003) [article on-line]; available from http://www.afcea.org/signal/articles/anmviewer.asp?a=168&z=49; Internet; accessed 17 April 2005.

[145] Edward Waltz, *Knowledge Management in the Intelligence Enterprise* (Boston, Massachusetts: Artech House Inc., 2003), 42.

interoperability again becomes key to a multinational force in sustaining a robust

information infrastructure to protect classified information stores, while enabling access

to the multitude of open information stores and databases.

Any "…combination of personnel, efforts, forms, instructions, procedures, data,

communication facilities and equipment that provides an organized and interconnected

means of displaying information in support of specific functions,"[146] is known as an

information system. However, the information gathered is merely a compilation of data

until it is filtered and categorized (synthesized)[147] by intelligence personnel, intelligence

management systems or in most cases both. This brings one to the third element in the

knowledge processing, in which information added into a system is then analyzed, sorted,

and clustered into groupings with meaning. In this step, data is presented to "…the

HUMINT analyst for examination using visualization tools to bring into focus the most

meaningful and relevant data items and their interrelationships."[148] At this point,

information is usually categorized into three groups: basic, current, and estimative

intelligence. The idea behind basic intelligence is to provide "…a full picture of a given

situation as possible, drawing on publicly available data and relevant information from all

intelligence sources."[149] For the military this might equate to specifics of an airbase, post

or naval station to include units assigned, capabilities, exercise schedules and other

---

[146] Defense Systems Management College (DMSC), *Glossary: Defense Acquisition Acronyms and Terms*, 6th Ed. (Fort Belvoir, Virginia: DMSC Press, March 1995), 69.

[147] Synthesized is a common term used to describe the combination of elements into an organized whole; additional information is located at: Catherine Soanes, *Pocket Oxford English Dictionary,* 9th ed. (Oxford, New York: Oxford University Press, Inc., 2002), 924.

[148] Edward Waltz, *Knowledge Management in the Intelligence Enterprise*, 44.

[149] Abram N. Shulsky and Gary J. Schmitt, *Silent Warfare: Understanding the World of Intelligence*, 60.

critical elements of the site operations. This information may contain both classified and unclassified information. For instance, any specific imagery taken by classified assets or information in which a classified source identity could be compromised would be strictly controlled.

From basic intelligence, one can then branch off into current intelligence, in which is focused on the real-time developments of a given situation. "The range of information that should be covered depends on the scope of the nation's intelligence interest."[150] Based on the nation's priorities, intelligence personnel will respectively narrow their collection to the highest priorities to satisfy political requests. Likewise, military intelligence analysts focus their collection to those top requirements necessary to support strategic, operational and tactical priorities. The greatest advantage to current intelligence is the "indicators" it may produce. Indications that a current intelligence report may identify include "…the calling up of reservists, forward movement of military forces, changes in communications patterns, and so forth."[151] These indicators may assist political and military leaders in quickly responding to changes in a given situation.

The last branch of basic intelligence is the estimative intelligence. National Intelligence Estimates (NIEs) "…are intended to help policymakers and warfighters think through key issues by presenting forward-leaning judgments about the likely course of events in foreign countries and their implications for the United States."[152] Suffice to

---

[150] *Ibid.,* 57.

[151] *Ibid.,* 59.

[152] Harold Brown, *Preparing for the 21st Century: An Appraisal of U.S. Intelligence* (Commission on the Roles and Capabilities of the United States Intelligence Community, March 1996) [report on-line]; available from http://www.access.gpo.gov/int/report.html; Internet; accessed 17 April 2005.

say, estimative intelligence provides both political and military leaders with a product

that "…not only describes the situation but also attempts to predict how it will evolve."[153]

Probably the most publicized NIE in recent history deals with the U.S. estimate of

Iraq's Weapons of Mass Destruction (WMD). Within the key judgments outlined in NIE

2002-16HC, analysts declared "Since inspections ended in 1998, Iraq has maintained its

chemical weapons effort, energized its missile program and invested more heavily in

biological weapons; in the view of most agencies, Baghdad is reconstituting its nuclear

weapons program."[154] Statements such as this would lend credibility to the case for

removing Saddam Hussein to protect regional forces. Additionally, the estimate states,

"Iraq would probably attempt clandestine attacks against the U.S. Homeland if Baghdad

feared an attack that threatened the survival of the regime were imminent or unavoidable,

or possibly for revenge."[155] Strong statements conjuring up 9-11 style attacks on home

soil lend credence to the campaign to remove the leadership of Iraq. To close out the key

judgments section, analysts stated with high confidence that "…Iraq possesses Proscribed

chemical and biological weapons and missiles."[156] Armed with hindsight, one can now

understand what potentially drove the "Coalition of the Willing" to action, but in the

aftermath, the complete lack of WMD evidence leans toward a failure in the estimate.

---

[153] Abram N. Shulsky and Gary J. Schmitt, *Silent Warfare: Understanding the World of Intelligence*, 60.

[154] United States, Director of Central Intelligence, "Iraq's Continuing Programs for Weapons of Mass Destruction," National Intelligence Estimate, NIE 2002-16HC (Washington, D.C.: Central Intelligence Agency, April 2004), 5.

[155] *Ibid.,* 8.

[156] *Ibid.,* 9.

How then should the knowledge sharing process attempt to minimize erroneous estimate reporting? This brings us to the next step to providing users the required decision-making information, the transition of intelligence into knowledge. Three major factors become pertinent in the transition from intelligence to knowledge: prioritization, objectivity and cultural understanding of intelligence.

Prioritization deals with the understanding the requirements and priority politicians and military leaders have on certain elements of intelligence. Most knowledge and intelligence systems allow a steady stream of inputs from "…counter-part bureaucracies, international organizations, and private sector parties pursuing their own agendas."[157] Classified intelligence can likewise lead to information overload, as many times classified information is "…afforded direct access to the decision-maker without being subject to in-depth staff scrutiny and proper integration with unclassified official and external information."[158] At this point, it is important to understand which intelligence products are relevant to the decision. The knowledge sharing system must provide the capacity to discriminate, distillate and then begin to disseminate information and intelligence products.

When and if politicians and military leaders set the information collection priorities, it then becomes reliant upon the intelligence agencies for collection and preparation of the situation.[159] By focusing efforts on the outlined priorities, intelligence

---

[157] Robert David Steele, *On Intelligence: Spies and Secrecy in an Open World* (Fairfax, Virginia: AFCEA International Press, May 2000), 128.

[158] *Ibid.,* 128.

[159] In Hulnick's passage on the intelligence process he points out just how difficult getting true prioritization from politicians can truly be. In most case it will be up to analysts to have a general understanding of what political leaders are looking for and then begin to develop intelligence products.

analyst can then began the process of objectively validating specific information

requirements through discrimination. Analysts must discriminate "…between valid and

invalid information, through the constant process of source validation, generally a labor-

intensive process requiring genuine human expertise as well as new developments in

automated understanding."[160] This is to say, "…every source should be clearly and

explicitly evaluated in terms of its authority, currency and confidence level."[161]

Following discrimination, analyst must then take the intelligence and begin to combine

research judgments and expert subject matter knowledge to distill the broader effort into

'just enough' intelligence to assist with a particular decision.[162] However, this is also

where subjectivity may creep back into the estimate process. "…Ideal intelligence work

would be objective, autonomous, and free of political pressures."[163] Realistically, amid

political pressures, analysts should still be afforded as much latitude to objectively

analyze source intelligence and attempt to provide unambiguous declarations as to the

indications present within the data, information and intelligence.

In performing an estimate, analysts must also take into account the cultural

differences that might be inherent within the context of the intelligence. Based on the

location and circumstances of a given situation, linguistic skill and area knowledge could

prove invaluable to the understanding of an adversary potential action. Subject matter

---

Arthur S. Hulnick, *Fixing the Spy Machine: Preparing American Intelligence for the Twenty-First Century*, 6.

[160] Robert David Steele, *On Intelligence: Spies and Secrecy in an Open World*, 175.

[161] *Ibid.*, 112.

[162] *Ibid.*, 175.

[163] Michael I. Handel, *War, Strategy and Intelligence* (London, England: Frank Cass and Company Limited, 1989), 189.

experts must understand both the language and the culture, as "…the greater the differences between languages' structure and culture, the greater the difficulty to accurately translate the intent of the speaker."[164] To exacerbate the situation further, "…languages are an expression of an individual's cultural, political, social, and religious experiences, even free translations of phrases can be difficult."[165] The fact that computers may only assist in simplistic translation brings about the requirement to ensure linguists that have sufficient area knowledge are fully integrated into the military knowledge sharing process to decipher the true meaning of military intelligence. "The point is that the linguist must also have the military intelligence skills of an experienced analyst to recognize the context of what might be meant."[166]

Once intelligence and information has been fused into a knowledge database, knowledge may then begin the process of dissemination to users and decision-makers. "No matter how much information is collected, processed, analyzed, and stored, intelligence is of no value unless it is available to combat commanders when they need it."[167] For decision-makers that have full security access to the host nation secure knowledge, the knowledge may only require delivery for consideration. However, not all members of multinational operations will have the same clearance and access as many of

---

[164] Dr. Clifford F. Porter, "Asymmetrical Warfare, Transformation, and Foreign Language Capability" (Combat Studies Institute Combined Arms Center Paper, April 2005) [paper on-line]; available from http://www.leavenworth.army.mil/csi/pubs/AsymmetricalWarfare.asp; Internet; accessed 17 April 2005.

[165] *Ibid.,* accessed 17 April 2005.

[166] *Ibid.,* accessed 17 April 2005.

[167] Captain Neal J. Wegner, "The Intel XXI Concept III: The Seven Intelligence Tasks," *Military Intelligence Professional Bulletin* (January – March 1997) [article on-line]; available from http://www.fas.org/irp/agency/army/tradoc/usaic/mipb/1997-1/cncp9701.htm; Internet; accessed 18 April 2005.

the host nation personnel, and yet will still require access to specific knowledge in

making decisions. To address this issue, one must again return to the argument for MLS

coupled with solid push-pull Information Assurance (IA) policies. As mentioned earlier

in this document MLS is critical to handling users with different access levels. "MLS

allows information with different sensitivities…to be stored and processed by users with

appropriate security rights, while preventing users from accessing information for which
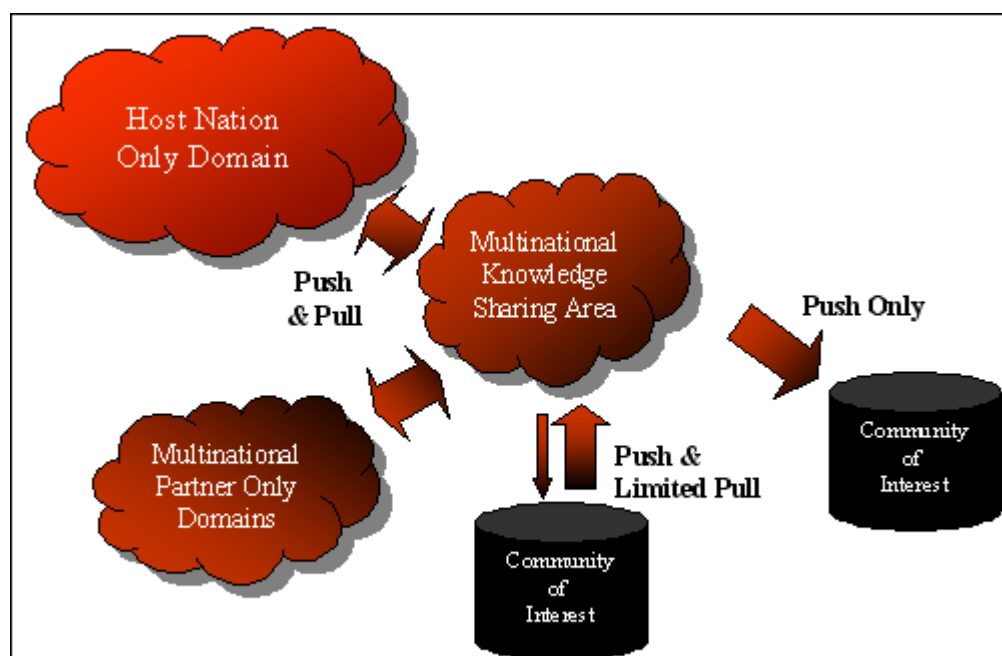
Figure 4-2. Knowledge Dissemination Process

they are not cleared."[168] MLS architectures provide lead nations with the ability to

provide both limited and restricted access to critical operations intelligence, as depicted

in figure 4-2.[169] Currently, the U.S. is expanding Multinational Information Sharing

---

[168] S.C. Spring, Dennis M. Gormley, K. Scott McMahon, Kenneth Smith, and Daniel Hobbes, *Information Sharing for Dynamic Coalitions*, Report prepared for the Air Force Research Laboratory (Arlington, Virginia: Pacific Sierra Research, December 2000), 9.

[169] Adapted depiction from the United States MNIS Protection Profile, for additional information see: Director National Security Agency, *Multinational Information Sharing (MNIS) Protection Profile (PP) For Networked Information Systems* (Fort Meade Maryland: U.S. Government Printing Office, September 2002), 21.

(MNIS) access with the advocacy of "…the MNIS Combined Enterprise Regional

Information Exchange System (MNIS CENTRIXS) as the DoD standard for

multinational information sharing networks using the Global Information Grid (GIG)."[170]

CENTRIXS allows the establishment of specified information domains to allow various

levels of assured access by multinational members. The top U.S.-Only Domain provides

exclusive access to "…U.S. Secret information restricted from distribution to non-U.S.

citizens and unauthorized U.S. citizens."[171] A second tier domain called the MNIS

Domain provides, as the name indicates multinational Secret Information and "…equates

to one or more environments consisting of people from both the U.S. and potentially all

partner nations, computers, software, networks and security devices, all of which help

compute and organize sharable information."[172] The third type of domain is similar to

the U.S. Only, but applies to other member states secret information, called Partner

National Domains. These domains contain "…foreign partner originated information that

is not releasable outside of the country of origin without further review."[173] The last sub-

domains established by CENTRIXS are Community Of Interest (COI) sub-domains. COI

sub-domains contain secret information that has been "…downgraded and released

information from the information domains of both the U.S.-only domain and the other

---

[170] Department of Defense, *Department of Defense Instruction, No. 8110.1: Multinational Information Sharing Networks Implementation*, (Washington, D.C.: U.S. Government Printing Office, February 2004), 1.

[171] Director National Security Agency, *Multinational Information Sharing (MNIS) Protection Profile (PP) For Networked Information Systems*, 20.

[172] *Ibid.,* 20.

[173] *Ibid.,* 20.

Partner National Domains."[174] By sanitizing specific intelligence, the knowledge system

can then share critical pieces of the information to additional multinational partners with

lower clearance levels. This concept was put to the test during Operation Iraqi Freedom

and as stated in the U.S. Navy's CHIPs Magazine, CENTRIXS "…allowed our coalition

partners and allies to leverage some of the same network-centric capabilities that we

benefit from."[175] What CENTRIXS and other multinational solutions aim to provide is

various levels of access through various levels of boundary protection or Information

Assurance (IA) techniques.

U.S. doctrine stipulates "IA protects and defends information and information

systems by ensuring their availability, integrity, identification and authentication,

confidentiality, and non-repudiation."[176] These five parameters are critical to ensuring

the right knowledge gets to the right individuals with the right clearance at the right time.

To share knowledge while maintaining IA, the system must be robust enough to support

the diversity of domain requirements and stringent security measures. The infrastructure

must provide network connectivity with "…global access to information and the ability to

pull or push information to all others connected to the network."[177]

One such construct is the U.S. Global Information Grid (GIG), in which the vision

"…is to empower users through easy access to information anytime and anyplace, under

---

[174] *Ibid.,* 20.

[175] Dennis M. Bauman, "Decision Superiority for the Joint Warfighter," CHIPs Magazine, Volume XXII, Issue 3 (Summer 2004): 9.

[176] Joint Chiefs of Staff, *Joint Publication3-13: Joint Doctrine for Information Operations* (Washington, D.C.: U.S. Government Printing Office, October 1998), III-1.

[177] Air Force Press Network (AFPN), "Airborne Network to Link Sensors, Shooters, Decision Makers," *Intercom*, Volume 46, No. 4 (April 2005): 19.

any conditions, with attendant security."[178] To support this vision, the GIG "…requires a comprehensive information capability that is global, robust, survivable, maintainable, interoperable, secure, reliable, and user-driven."[179] This is to say the Global Information Grid must be developed jointly to fully appreciate the synergies it can create amongst the components. In effect, the GIG should provide the worldwide "…end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel."[180] This system is designed to provide the backbone for U.S. Armed Forces communications and information. Therefore the system must focus on two areas outlined by the DoD. The first deals with future acquisitions in information technologies, in which investment must focus on "…core [GIG] enterprise programs and initiatives to build a core network and information capability."[181] In other words, new programs must take into account the GIG vision and design systems that will interoperate with the GIG infrastructure. The second aspect deals with legacy and current programmed projects. The DoD stipulates that systems, to include "…existing and planned weapon systems, command, control, and communications systems, information technology systems, and logistics, personnel, and other business-related systems,"[182]

---

[178] United States, Defense Acquisition University, "Defense Acquisition Guidebook," http://akss.dau.mil/dag/; Internet; accessed 13 March 2005, Para. 7.2.1.1.

[179] *Ibid.,* Para. 7.2.1.1.

[180] United States, Department of Defense, *Department of Defense Directive Number 8100.1: Global Information Grid Overarching Policy*, 8.

[181] Government Accountability Office, *The Global Information Grid and Challenges Facing Its Implementation* (House of Representatives Subcommittee on Terrorism, Unconventional Threats, and Capabilities, Committee on Armed Services Report, July 2004), 8.

[182] *Ibid.,* 8.

should be brought under the GIG umbrella. By building a joint, integrated infrastructure theater forces will, with the appropriate bandwidth, be able to increase efficiency by reducing redundant infrastructure requirements. From this construct one can begin to imagine the potential advantages of applying sound Multinational MLS and CENTRIXS practices to the GIG to expand this global connectivity to multinational partners on demand.

There is no doubt that "…knowledge is indeed power, but only if the knowledge is findable, accessible, and useable."[183] Therefore, throughout this section the knowledge sharing process was examined to identify the key requirements of each step in the knowledge sharing process. From the external and internal sources input through to the dissemination of synthesized knowledge and intelligence products, the recurring themes of interoperability, need for language understanding, and the sanitizing of intelligence for lower level release has continued to remain critical elements to effective knowledge sharing.

---

[183] Intelligence Community Metadata Working Group (IC MWG), *Metadata and XML: Defining a New Intelligence Paradigm* (April 2003), accessed 13 April 2005.

SECTION 5

KNOWLEDGE SHARING IN THE BATTLESPACE

> Wartime campaigns integrate air, land, sea, space and special operations, interagency and multinational operations in harmony with diplomatic, economic, and informational efforts to attain national and multinational objectives.
> – US Air Force Doctrine Document 2-1

So what progress has been made to begin building towards multinational knowledge sharing systems at the theater level of operations "where the rubber meets the road" so to speak? "Intelligence sharing and interoperability are essential for responsiveness and dominance on the battlefield."[184] If concepts and systems are to become true information superiority enablers, they must provide adaptability for use in multinational operations. Equally, they must be flexible, mobile, easy-to-use, all while remaining survivable and secure. This section will first address the conceptual notion of Network-Centric Warfare (NCW). After understanding the framework, analysis will shift to the Command, Control, and Communications (C3) and Mission Support systems that are currently being developed and fielded with consideration for both joint and multinational operations. Through examination of these systems it will be illustrated that not only is knowledge sharing a possibility, but also a reality for those willing to dedicate resources to it.

---

[184] Major Michele H. Bredenkamp, "How Can the U.S. Army Overcome Intelligence Sharing Challenges Between Conventional and Special Operations Forces," 7.

Network-Centric Warfare

> The net-centric environment is a framework for full human and technical connectivity that allows all DoD users and <u>mission partners</u> to share the information they need, when they need it, in a form they can understand and act on with confidence; and protects information from those who should not have it.
> - DoD Network Centric Environment Joint Functional Concept

Network-Centric Warfare is designed to build on the GIG infrastructure and create "…capabilities for unparalleled information sharing and collaboration, adaptive organizations, and a greater unity of effort via synchronization and integration of force elements at the lowest levels."[185] By utilizing the common GIG infrastructure, the users can begin to draw upon this technical interconnectivity to share information and knowledge. "If the Joint Force fully exploits both shared knowledge and technical connectivity, then the resulting capabilities will dramatically increase mission effectiveness and efficiency."[186] This knowledge sharing creates an environment for joint collaboration on operations, or a collaborative information environment (CIE). CIE allows both theater forces and reachback forces to interact within a single network environment to "…to create and share the data, information, and knowledge needed to plan, execute, and assess joint force operations and to enable a commander to make decisions better and faster than the adversary."[187] The question then becomes one of whether or not to expand this capability to multinational partners.

---

[185] Department of Defense, *Network Centric Environment Joint Functional Concept* (Washington, D.C.: U.S. Government Printing Office, November 2004), v.

[186] *Ibid.,* 10.

Recent operations in Iraq provide strong justification for the need to implement knowledge sharing systems within multinational operations. During Operation Iraqi Freedom, "…coalition assets reportedly operated as separate entities, and coalition forces were often locked out of planning and execution because most information was posted on systems accessible only to U.S. forces."[188] Although some manual processes were put into place to provide multinational members with some degree of information, the synergies that can be provided by NCW were effectively nullified due to security requirements.

As Col Chekan points out, there are three basic risks associated with bringing multinational members under the NCW umbrella: 1) the risk that technologies would be compromised; 2) the risk that less technologically developed coalition members will introduce vulnerabilities to the system; and 3) the risk that degrading the information architecture would have the largest impacts on the U.S. itself.[189] Since, in Col Chekan's words "…Network-Centric Warfare is fundamentally different than any warfare that has preceded it because it intends to operate in real-time using all sources of information to establish unprecedented battlespace awareness,"[190] the perceived risk to security is justifiable. However, with security as the paramount concern, by incorporating solid MLS or CENTRIXS technology, the risks associated with knowledge sharing can be

[187] United States, The Joint Warfare Center, *Joint Doctrine Series Pamphlet 5: Operational Implications of the Collaborative Information Environment (CIE)* (Washington, D.C.: U.S. Government Printing Office, June 2004), 5.

[188] Clay Wilson, *Network Centric Warfare: Background and Oversight Issues for Congress,* CRS Report for Congress (Washington, D.C.: The Library of Congress, Technology and National Security Foreign Affairs, Defense, and Trade Division), CRS-24.

[189] Colonel Robert Chekan, "The Future of Warfare: Clueless Coalitions?" (Toronto: Canadian Forces College Advanced Military Studies Course Paper, 2001), 10.

[190] *Ibid.,* 7.

minimized. U.S. projects such as Horizontal Fusion, also known as the Network Centric

Enterprise Service (NCES), focus on providing "…information immediately available to

any coalition partners who need it, while also providing strong security through network

encryption technologies and dynamic access controls."[191] By providing multinational

partners restricted secure access to information, the U.S. can extend knowledge sharing to

multinational partners and synergize the effectiveness of the total force.

Bearing in mind the principles associated GIG and NCW; one can then begin to

explore the theater systems currently deployed to field units or under development. "To

be successful operationally, a clear understanding of the national and military strategic

goals and objectives is required."[192] To this end, probably the most important area for

consideration of a multinational operation is command and control. Each multinational

member state will require clear guidance and direction as to what specific objectives they

are assigned so as to dedicate assets and effectively contribute to the operation.

Currently, there are two major concepts or systems that merit acknowledgment. The first

such system is the Joint Command and Control (JC2) capability. JC2 is focused on

providing "…force-level planning, execution and assessment activities in support of joint,

allied and coalition operations."[193] This new capability will replace the current Global

Command and Control System (GCCS), moving to "…Web services and mesh with

DoD's demand for network-centric warfare capabilities."[194] GCCS provides a viable

---

[191] Clay Wilson, *Network Centric Warfare: Background and Oversight Issues for Congress*, CRS-24 and CRS-25.

[192] Colonel C.J.R. Davis, "Command and Control in Coalition Operations," 5.

[193] Defense Information Systems Agency (DISA), "Joint Command and Control (JC2)," http://www.les.disa.mil/c/extranet/home?e_l_id=33; Internet; accessed 14 March 2005.

template from which to work from; however, it can no longer keep up with the volume of applications and database requirements to move into the network-centric environment. "GCCS limitations stem from the fact that each military Service found it necessary to produce a tailored version of GCCS to support individual Service missions."[195] JC2 will enhance the common capabilities inherent in all component GCCS's, as well as, migrate to become the overarching joint command and control system at home and abroad for U.S. forces. The system "…is being designed for the Joint Force Commander to address mission areas in complete packages, for example, situation awareness and force protection instead of Service-centric tasks."[196] However, JC2 is not only being developed with joint interoperability in mind, but also with multinational accessibility as well. "JC2 will use Net-Centric Enterprise Services (NCES) Core Enterprise Services (CES) and will be able to exchange data across multiple security domains."[197] By incorporating MLS and CENTRIXS principles for security, the system can be configured to allow controlled multinational access.

The second command and control capability, Blue Force Tracking (BFT), has the potential to reduce the probability of fratricide. Aircraft have long been using Identification Friend or Foe (IFF) systems, but "Ninety percent of fratricides, however,

---

[194] Thomas Temin, "DoD to shelve GCCS, Roll Out New System," Government Computer News (26 April 2004) [article on-line]; available from http://www.gcn.com/23_9/news/25684-1.html

are of the ground-force-on-ground-force variety,"[198] making a BFT capability important

across the spectrum of joint and multinational warfare. U.S. and allied forces in the

future will require the capability to track all forces within the theater of operations. The

current U.S. BFT system aided immensely during Operation Iraqi Freedom, allowing

"…commanders and troops to distinguish between friend and foe and know at all times

where allied forces were located."[199] To do this, the Joint Blue Force Situational

Awareness (JBFSA) program is designed to integrate several component initiatives into a

single system for tracking all friendly forces in theater. JBFSA, in conjunction with the

Joint Translator Forwarder (JxF) and Rapid Attack Information Dissemination Execution

Relay (RAIDER), will be linked into the overall theater Combat Identification (CID)

program allowing commanders to monitor "…multiple blue force tracking systems

operating within his assigned area, and identify the tracked friendly forces, thus reducing

the likelihood of blue-on-blue engagements."[200] However, there is much work to be done

in integrating joint and multinational BFT systems. In Iraq, "…units in theater arrived

with seven different combat identification systems, and our commanders were forced to

overcome these shortcomings, 'on the fly,'"[201] let alone the differences in multinational

partner systems. Even the U.S. closest partner in the conflict, Great Britain struggled to

---

[198] George Cahlink, "Better 'Blue Force' Tracking," *Air Force Magazine Volume* 87, no. 6 (June 2004): 68.

[199] Frank Tiboni and Matthew French, "Blue Force Tracking Gains Ground," Federal Computer Weekly (22 March 2004) [article on-line]; available from http://www.fcw.com/fcw/articles/2004/0322/tec-blueforce-03-22-04.asp; Internet; accessed 17 March 2005.

[200] Lieutenant General Robert W. Wagner, *C4 Systems and the Role of U.S. Joint Forces Command in Developing a "Coherently Integrated Joint Force,"* (House of Representatives House Armed Service Committee Subcommittee Terrorism, Unconventional Threats and Capabilities Statement, March 2005), 10.

[201] Anthony H. Cordesman, *The Lessons of the Iraq War: Executive Summary*, (Center for Strategic and International Studies (CSIS) Paper, July 2003), 7.

find the utility of the system. "One British HQ reported that the most important use of BFT was to display the location of US forces theatre-wide, providing a broad situation report."[202] Brigadier General Dennis C. Moran of the U.S. Army Central Command (CENTCOM) staff reportedly stated that the "…differences encompassed both capabilities and techniques, tactics and procedures."[203] To resolve many of the issues, liaison officers were called in to provide multinational support. "Gen. Moran relates that, at the division, corps and coalition forces land component command levels, the command had to work hard with tried-and-true interoperability methods such as liaison officers (LNOs)… to share information seamlessly with our coalition partners."[204] This therefore points out two critical aspects to implementing multinational BFT. First, the system must provide interoperability to legacy and international systems; and second this once again reinforces the argument for early involvement of liaison officers to ascertain multinational partner capabilities and potential integration options.

Global Positioning System (GPS) III is a new capability being designed to enhance the current GPS features. Although, there is discussion as to the initial launch dates of the first satellite, this new generation of satellites "…will include all of the legacy capabilities, plus the addition of high-powered, anti-jam military-code, along with

---

[202] Lieutenant Colonel J.P. Storr, PhD, The Command of British Land Forces in Iraq, March to May 2003 (2003) [report on-line]; available from http://www.dodccrp.org/events/2004/ICCRTS_Denmark/CD/papers/068.pdf; Internet; accessed 16 April 2005.

[203] Robert K. Ackerman, "Iraq War Operations Validate Hotly Debated Theories," *Signal Magazine* (July 2003) [article on-line]; available from http://www.afcea.org/signal/articles/anmviewer.asp?a=105&z=57; Internet; accessed 20 April 2005.

[204] *Ibid.,* accessed 20 April 2005.

other accuracy, reliability, and data integrity improvements."[205] GPS III will expand the

current use of positioning information in land, sea, and air forces tracking and precision

guided munitions delivery. GPS is also a key factor in low visibility landings for aircraft.

The new GPS III constellation would "…virtually eliminate the position errors produced

by random and unpredictable ionospheric activity."[206] This capability could virtually

eliminate the need for many of the instrument landing systems (ILS) used both in civil

and military aviation. By negating the need for bulky ILS system support equipment this

would reduce the military footprint required for austere locations. Multinational use of

GPS technology is already in use in many locations; however, to enhance the anti-

jamming features some equipment will require upgraded system components.

Command and Control aside, the next critical area is communication between

forces. From the interconnectivity of ground to air, air to sea or any other combination of

the three, to interconnectivity of coalition forces in any of the environments, all have

significant need of reliable wireless communications. To accommodate this requirement

the Joint Requirements Oversight Committee (JROC) approved work to establish the

Joint Tactical Radio System (JTRS) to "…combine the functionality of numerous single

function radios among the services into a single, Joint-interoperable family of radios."[207]

---

[205] Peter B. Teets, *Regarding the Fiscal Year 2005 National Defense Authorization Budget Request: Status of the Space Programs* (House Armed Services Committee Statement by the Undersecretary of the Air Force, February 2004) [statement on-line]; available from http://armedservices.house.gov/openingstatementsandpressreleases/108thcongress/04-02-25teets.html; Internet; accessed 15 March 2005.

[206] William Reynish, "AU.S. Embarrassment?" *Aviation Today* (17 March 2005) [article on-line]; available from http://www.aviationtoday.com/cgi/av/show_mag.cgi?pub=av&mon=0902&file=0902viewpoint.htm; Internet; accessed 17 March 2005.

The system will be designed with internal cryptographic features to ensure system integrity and security. However, the cryptographic feature will not preclude the system from interoperating in a coalition environment. In fact, the system will "…attain Joint, Federal Agencies and Public Safety, Combined, and Allied/Coalition interoperability and performance requirements."[208] This system will provide functionality and service for operational and combat support personnel alike. In fact, "…it is being scaled for use in all domains: airborne, ground, mobile, handheld, fixed station, maritime, civilian and personal."[209] The development of JTRS is keeping interoperability at the forefront by designing the system with "…common communications system architecture— interoperable with legacy communications systems and capable of accepting future technology insertions."[210] Thereby it can provide functionality in some multinational settings. The United Kingdom has already embraced the idea of a single family of products to promote greater interoperability. In June of 2004, during a demonstration at the British embassy in Washington, D.C., engineers passed secure voice and data between the British Bowman radio and the new U.S. Joint Tactical Radio System (JTRS)."[211]

---

[207] United States, Joint Requirements Oversight Council, *Joint Tactical Radio System (JTRS) Operational Requirements Document (ORD), Version 3.2* (Washington, D.C.: U.S. Government Printing Office, April 2003), 1.

[208] *Ibid.,* 1.

[209] Captain Steven T. Wall, "Joint Tactical Radio System: Volume, Distance and Speed," *Field Artillery Journal*, HQDA PB 6-00-1 (Fort Sill, Oklahoma: U.S. Field Artillery Association, January-February 2000), 45.

[210] *Ibid.,* 45.

[211] Nicole A. Manara, "Military Trends in the United Kingdom: Strengths and Weaknesses," *Center for Strategic and International Studies (CSIS)* (Washington, D.C.: CSIS, August 2004), 14.

The next communications capability worth exploring, entitled Transformational

Satellite (TSAT), intends to provide the infrastructure necessary for U.S. voice, data, and

imagery access anywhere and anytime. Following Operation Enduring Freedom, the

United States Air Force reported, "…that the demand for communications bandwidth

increased 473 percent between Operation Desert Storm in 1991 and Operation Enduring

Freedom in 2001."[212] As a key component of the future GIG architecture, TSAT is

designed to not only provide a significant increase in access, but also provide on-demand

Intelligence, Surveillance and Reconnaissance (ISR) and Battle Damage Assessment

(BDA). As the DoD's premiere satellite system for the future; "…space, air, land, and

sea-based systems will depend on TSAT to receive and transmit large amounts of data to

each other as DOD moves toward a more network centric war-fighting approach."[213]

This capability has numerous uses across the spectrum of forces, to include multinational

partners who are granted access to network resources NCES and CENTRIXS.

The last area to address is that of combat support, or those functions (Logisticians

and Support Functions) that provide enabling services that are critical to operational

success. Many of these elements have historically operated independently. However, to

meet the challenges of modern warfare, these functions need to be "…integrated to create

a systematic process for providing seamless combat support while minimizing the

support footprint."[214] To achieve this across the services, the Global Combat Support

---

[212] Robert E. Levin, *Space Acquisitions: Committing Prematurely to the Transformational Satellite Program Elevates Risks for Poor Cost, Schedule, and Performance Outcomes*, Memorandum Prepared for the Secretary of Defense (Washington, D.C.: General Accounting Office, December 2003), 3.

[213] Robert E. Levin, *Improvements Needed in Space Systems Acquisition Policy to Optimize Growing Investment in Space*, U.S. Senate Subcommittee on Strategic Forces, Committee on Armed Services Testimony (Washington, D.C.: General Accounting Office, November, 2003), 2.

System (GCSS) has been designed by the United States Air Force for use in the joint arena. The GCSS capability "…provides the warfighter with a single, end-to-end capability to manage and monitor units, personnel and equipment through all stages of the mobilization process."[215] This capability is critical to tracking and providing those required services personnel, products and equipment to theater as needed. This application is equally applicable to multinational forces and their required combat support. To accommodate the combat support requirements of multinational forces, the GCSS program office, in coordination with the Defense Information Systems Agency (DISA) and Australia is working to design a GCSS combat support technology for all multinational members through the Coalition Theater Logistics (CTL) concept. Although still in the proving stages, CTL will provide multinational logistics information, logistics analysis, interoperability to coalition systems, and interactive tools to assist with deployment, execution, sustainment and redeployment decisions.[216] This concept is specifically designed for multinational operations and will most likely be developed under future iterations of the GCSS capability.

In this section, several major initiatives or concepts undertaken by U.S. forces have been outlined. Progress towards coalition interoperability is being made in command, control, communications and various aspects of the combat support. To further illustrate the desire of the United States to continue to operate in multinational

---

[214] Secretary of the Air Force, *Air Force Doctrine Document 2-4: Combat Support* (Washington, D.C.: U.S. Government Printing Office, November 1999), 4.

[215] United States, Defense Information Systems Agency (DISA), "Global Combat Support System (GCSS) Combatant Commanders/ Joint Task Force (CC/JTF)," accessed 17 March 2005.

[216] United States, Department of Defense, *Coalition Theater Logistics Advanced Concept Technology Demonstaration (CTL-ACTD) Management Plan*, (Washington, D.C.: U.S. Government Printing Office, November 2001), 2.

environments, one need only look to the nation's current National Defense Strategy which states, "We will help partners increase their capacity to defend themselves and collectively meet challenges to our common interests."[217] To accomplish this, the United States must continue to maintain its technological edge, but develop that edge keeping its potential partners in mind. By developing systems such as JC2, JBFSA and GPS III compatible to the common GIG and NCW concepts, the U.S. is making tremendous efforts toward striking a balance between sharing critical information with multinational partners, while maintaining system integrity and security. Likewise, although machine-to-machine crosstalk provides far greater speed, there is still a need for human liaison officers, as in the case with BFT in Iraq. Failure to design systems with multinational interoperability will only create greater disparities in technology and hamper the ability of other national forces to make effective contributions to U.S. led operations. Systems must be designed to provide not only joint forces the appropriate knowledge to accomplish tasks, but also provide that same level of service to multinational partners.

---

[217] Donald H. Rumsfeld, *The National Defense Strategy of the United States of America* (Washington, D.C.: U.S. Government Printing Office, March 2005), iv.

SECTION 6

CONCLUSION

Throughout this document interoperability, language and the sharing of intelligence have played a key role in determining the effectiveness of knowledge sharing in a multinational environment.   The ability to share knowledge has and will likewise continue to play a critical role to the successful deployment and engagement of multinational forces.   In each of the historical examples, the forces that discovered ways to work around disparities within the three detriments met with greater results. In those instances where the multinational forces failed to accurately address the determinants, friction such as misdirection or fratricide was more likely to occur. Therefore effective consideration of the determinants and the ability to share knowledge between national forces did contribute to the level of operational success.

In analyzing the delineation between allied and coalition forces, it became clear that systems must not be designed for just one set of partners or another, but as a multinational system capable of meeting the requirements of various nations with different levels of capability.

From black and white signal flags to the advent of wireless communications to the full spectrum of Global Information Grid and Network-Centric Warfare development projects, interoperability has remained a paramount concern in multinational operations. Without multinational interoperability, there is no guarantee that the right information will be delivered to the right individual at the right time to service targets or make

judgment calls as in the case of the A-10 over Iraq. In the end, interoperability basically

provides the infrastructure and processes necessary to exchange knowledge with others.

Language skill and cultural understanding has additionally played a pivotal part in

the history of multinational operations. As we look from Sir Robert the Bruce acting as a

liaison officer between his forces with different languages to the introduction of liaison

officers into foreign command centers to aid in interpreting decision-making knowledge,

one can easily predict that the importance of liaison officers will not waver. By

providing forces that can speak and understand other multinational partners, a lead nation

can ensure that the message they are sending is received as intended.

Finally, the ability to sanitize and share critical pieces of knowledge and

intelligence with multinational partners cannot be overstated. Ultimately, "…fighting our

enemies depends on information sharing and unencumbered access to the nation's

intelligence knowledge by those who need to know."[218] Interoperability may provide the

right connectivity and liaison officers can ensure the right translation, but it is the ability

to dissemination the right knowledge to multinational members that can ultimately help

both political and military leaders make informed decisions.

Therefore it is incumbent upon those lead nations, like the U.S., that are currently

developing knowledge sharing capabilities to clearly understand the implications

associated with interoperability, language, knowledge release and security to be

successful. Command and control programs like the JC2 and JBFSA, and for that matter

any crosscutting information and intelligence platforms must be deployed with

---

[218] Intelligence Community Metadata Working Group (IC MWG), *Metadata and XML: Defining a New Intelligence Paradigm*, (Technical Series, April 2003) [article on-line], accessed 13 April 2005.

multinational mindset as early in the acquisition process as possible. It's no longer a

question of whether or not to knowledge share, but now the degree to which

multinational forces must share to collectively contribute to the theater operation.

APPENDIX A

List of Acronyms

AAP	Allied Administrative Publication
ABCA	American, Britain, Canada, Australia Program
BDA	Battle Damage Assessment
BFT	Blue Force Tracking
C3	Command, Control and Communications
C4I	Command, Control, Communications, Computers and Intelligence
CENTCOM	Central Command
CENTRIXS	Combined Enterprise Regional Information Exchange System
CES	Core Enterprise Services
CID	Combat Identification
CIE	Collaborative Information Environment
COI	Community of Interest
COMINT	Communications Intelligence
CTL	Coalition Theater Logistics
DISA	Defense Information Systems Agency
DoD	Department of Defense
ELINT	Electromagnetic Radiation Intelligence
EOB	Electronic Order of Battle
GCCS	Global Command and Control System

GCSS	Global Combat Support System
GIG	Global Information Grid
GPS III	Global Positioning System III
HQ	Headquarters
HUMINT	Human Intelligence
IA	Information Assurance
IFF	Identification Friend or Foe
ILS	Instrument Landing System
IMINT	Imagery Intelligence
ISR	Intelligence, Surveillance and Reconnaissance
JBFSA	Joint Blue Force Situational Awareness
JBFT	Joint Blue Force Tracking
JC2	Joint Command and Control
JROC	Joint Requirements Oversight Committee
JTRS	Joint Tactical Radio System
JxF	Joint Translator Forwarder
LNO	Liaison Officer
MASINT	Measurement and Signatures Intelligence
MLS	Multilevel Security
MNIS	Multinational Information Sharing
NATO	North Atlantic Treaty Organization
NCES	Network-Centric Enterprise Services
NCW	Network Centric Warfare

NIE	National Intelligence Estimates
OAS	Organization of American States
PHOTINT	Photographic Intelligence
POW	Prisoner of War
RAIDER	Rapid Attack Information Dissemination Execution Relay
SIGINT	Signals Intelligence
TELINT	Telemetry Intelligence
TSAT	Transformational Satellite
UAV	Unmanned Aerial Vehicles
UTERM	United Nations Multilingual Terminology Database
WMD	Weapons of Mass Destruction
WWI	World War I
UN	United Nations
US or U.S.	United States

BIBLIOGRAPHY

Akerman, Robert K. "Advanced Surveillance Spawns New Challenges." *Signal Magazine* (March 2004). Article on-line; available from http://www.afcea.org/signal/articles/anmviewer.asp?a=28&z=10; Internet; accessed 16 April 2005.

Akerman, Robert K. "Document Exploitation Increases in Importance." *Signal Magazine* (August 2003). Article on-line; available from http://www.afcea.org/signal/articles/anmviewer.asp?a=168&z=49; Internet; accessed 17 April 2005.

Ackerman, Robert K. "Iraq War Operations Validate Hotly Debated Theories." *Signal Magazine* (July 2003). Article on-line; available from http://www.afcea.org/signal/articles/anmviewer.asp?a=105&z=57; Internet; accessed 20 April 2005.

American-British-Canadian-Australian (ABCA) Program. *ABCA Coalition Operations Handbook*. Washington, D.C.: U.S. Government Printing Office, November 2001.

Arthurson, Ian. "Espionage and Intelligence from the War of the Roses to the Reformation." *Nottingham Medieval Studies*, Version 35 (1991). Article on-line; available from http://www.deremilitari.org/RESOURCES/ARTICLES/nottinghammedievalstudies.htm; Internet; accessed 3 April 2005.

Ashworth, Tony. *Trench Warfare 1914-1918: The Live and Let Live System*. New York, New York: Holmes& Meier Publishers, Inc., 1980.

Bauman, Dennis M. "Decision Superiority for the Joint Warfighter." CHIPs Magazine, Volume XXII, Issue 3 (Summer 2004): 6-9.

Boardman, Jill L. "Combined Enterprise Regional Information Exchange System (CENTRIXS); Supporting Coalition Warfare World-wide." http://www.dodccrp.org/events/2004/ICCRTS_Denmark/CD/papers/003.pdf; Internet; accessed 7 April 2005.

Book, Elizabeth G. "Are Europeans willing to invest in interoperability?" *National Defense Magazine*, Volume 87, Iss. 589 (December 2002): 34-35.

Bredenkamp, Major Michele H. "How Can the U.S. Army Overcome Intelligence Sharing Challenges Between Conventional and Special Operations Forces?" United States Army Command and General Staff College School of Advanced Military Studies, 2002-2003.

British Broadcasting Corporation. "The Auld Alliance 1295."
    http://www.bbc.co.uk/history/timelines/scotland/auld_all.shtml; Internet; accessed
    26 March 2005.

British Broadcasting Corporation. "The Auld Alliance – Scotland and France."
    http://www.bbc.co.uk/history/scottishhistory/europe/features_europe_auldalliance
    .shtml; Internet; accessed 3 April 2005.

Brown, Harold. *Preparing for the 21st Century: An Appraisal of U.S. Intelligence.*
    Commission on the Roles and Capabilities of the United States Intelligence
    Community, March 1996. Report on-line; available from
    http://www.access.gpo.gov/int/report.html; Internet; accessed 17 April 2005.

Cahlink, George. "Better 'Blue Force' Tracking." *Air Force Magazine Volume* 87, no. 6
    (June 2004): 66-69.

Cerone, First Lieutenant Michael C. "Multilevel Network Security." *Hill Air Force Base
    Crosstalk* (September 1995). Article on-line; available from
    http://www.stsc.hill.af.mil/crosstalk/1995/09/Multilev.asp; Internet; accessed 20
    March 2005.

Chekan, Colonel Robert. "The Future of Warfare: Clueless Coalitions?" Toronto:
    Canadian Forces College Advanced Military Studies Course Paper, 2001.

Cirincione, Joseph, Jessica T. Mathews, George Perkovich and Alexis Orton. *WMD in
    Iraq: Evidence and Implications*. Washington, D.C.: Cambridge Endowment for
    International Peace, 2004.

Command, Control, Communications Computers, Intelligence, Surveillance, and
    Reconnaissance (C4ISR) Modeling and Simulation Branch. *Integrated Decision
    Systems: Command and Control of the Future.* Rome New York: Rome,
    Laboratories, April 2004. Article on-line; available from
    http://www.afrlhorizons.com/Briefs/Apr04/IF0315.html; Internet; accessed 20
    March 2005.

Cordesman, Anthony H. *The Lessons of the Iraq War: Executive Summary.* Center for
    Strategic and International Studies (CSIS) Paper, July 2003.

Cromwell, Bill. *Too Many Secrets: Overclassification as a Barrier to Critical
    Information Sharing.* Testimony Before the Subcommittee on National Security,
    Emerging Threats, and International Relations House Committee on Government
    Reform August 2004.

Daniels, Colonel George E. "An Approach to Reconnaissance Doctrine," *Air University
    Review*, March-April 1982. Air University Air War College Paper, 1982. Paper

on-line; available from
http://www.airpower.maxwell.af.mil/airchronicles/aureview/1982/mar-apr/daniels.html; Internet; accessed 13 April 2005.

Davis, Colonel C.J.R. "Command and Control in Coalition Operations." Toronto: Canadian Forces College Advanced Military Studies Course Paper, 2000.

Dizard, Wilson P., III. "Feds Expect XML to Ease Info Exchanges." *Government Computer Weekly*, Volume 21, No. 25 (August 2002). Article on-line; available from http://www.gcn.com/21_25/news/19780-1.html; Internet; accessed 31 March 2005.

Dupuy, R. Ernest and Trevor N. Dupuy. *The Encyclopedia of Military History from 3500 B.C. to the Present*, 2nd ed. Toronto, Canada: Harper and Row Publishers, Inc., 1986.

Eby, Gunner J.L. "I Told You So." *2nd Battalion, 5th Marines Website*. Article on-line; available from http://www.2ndbn5thmar.com/oif/told%20you%20so.htm; Internet; accessed 7 April 2005.

Encyclopedia Britannica Online. "Military Communications: From World War I to 1940." http://nasaa-home.org/history/his5comms.htm; Internet; accessed 6 February 2005.

Ford, Nancy Gentile. *Americans All! Foreign-born Soldiers in World War I*. College Station, Texas: Texas A&M University Press, 2001.

Fox, Lieutenant Colonel Steven J. "Unintended Consequences of Joint digitization." *Sun Tzu Art of War in Information Warfare*. National Defense University Institute for International Studies, 2002. Chapter on-line; available from http://www.ndu.edu/inss/siws/cont.html; Internet; accessed 8 April 2005.

Gardner, Nikolas. *Trial By Fire: Command and the British Expeditionary Force in 1914*. Westport, Connecticut: Praeger Publishers, 2003.

Gardner, Squadron Leader Sophy. "Operation Iraqi Freedom: Coalition Operations." *Air & Space Power Journal,* Volume XVIII, No. 4 (Winter, 2004): 87-99.

Gaurdian Unlimited. "Wounded British soldiers condemn US 'cowboy' pilot." http://www.guardian.co.uk/Iraq/Story/0%2C2763%2C926237%2C00.html; Internet; accessed 7 February 2005.

Gilbert, Adrian. *The Encyclopedia of Warfare From the Earliest Times to the Present Day*. Chicago, Illinois: Fitzroy Dearborn Publishers, 2000.

Gunn, R.M. "The Bruce Bannockburn and Beyond." *AOL.Hometown* (2003). Available from http://members.aol.com/skyelander/bruce1.html; Internet; accessed 3 April 2005.

Gunn, R.M. "William the Lion of Scotland." *AOL.Hometown* (2003); available from http://members.aol.com/skyewrites/thelion.html; Internet; accessed 1 February 2005.

Handel, Michael I. *War, Strategy and Intelligence.* London, England: Frank Cass and Company Limited, 1989.

Hulnick, Arthur S. Fixing the Spy Machine: Preparing American Intelligence for the Twenty-First Century. Westport Connecticut: Praeger Publishers, 1999.

Intelligence Community Metadata Working Group (IC MWG). *Metadata and XML: Defining a New Intelligence Paradigm* (April 2003). Article on-line; available from https://www.xml.saic.com/icml/xnotes/MetadataXML/MetadataXML.html; Internet; accessed 13 April 2005.

Johnson, Steven. "Military Public Relations in the Americas: Learning to Promote the Flow." Center for Hemispheric Defense Studies Research and Education in Defense and Security Studies Paper, May 2001.

Kasturi, Bhashyam. "Military Intelligence in India: An Analysis" (1995). Article on-line; available from http://www.bharat-rakshak.com/LANCER/idr00001.htm; Internet; accessed 2 April 2005.

Keuhlan, Captain Daniel T. (USN). *The Common Operating Picture in Joint Vision 2020: A Less Layered Cake*. Joint Forces Staff College Research Paper, May 2002.

Kusnetz, Marc, William M. Arkin, General Montgomery Meigs (Retired), and Neal Shapiro. *Operation Iraqi Freedom.* Kansas City, Missouri: Andrews McNeel Publishing, 2003.

Levin, Robert E. *Improvements Needed in Space Systems Acquisition Policy to Optimize Growing Investment in Space*. U.S. Senate Subcommittee on Strategic Forces, Committee on Armed Services Testimony. Washington, D.C.: General Accounting Office, November, 2003.

Levin, Robert E. *Space Acquisitions: Committing Prematurely to the Transformational Satellite Program Elevates Risks for Poor Cost, Schedule, and Performance Outcomes.* Memorandum Prepared for the Secretary of Defense. Washington, D.C.: General Accounting Office, December 2003.

Lowenthal, Mark M. *U.S. Intelligence: Evolution and Anatomy*, 2nd ed. Westport, Connecticut: Praeger Publishers, 1992.

Manara, Nicole A. "Military Trends in the United Kingdom: Strengths and Weaknesses." *Center for Strategic and International Studies (CSIS).* Washington, D.C.: CSIS, August 2004.

Mcginnis, Lieutenant Colonel Robert L. (Retired). "Keeping our Best Army Coalition Relevant by Transforming Together." *Army Magazine* (September 2003). Article on-line; available from http://www.ausa.org/www/armymag.nsf/0/003C39EC1847B53185256D8600612 11F?OpenDocument; Internet; accessed 20 March 2005.

Miller, Eric S. "Interoperability of Rules of Engagement in Multinational Maritime Operations." Center for Naval Analyses Research Memorandum, October 1995.

Mitchell, Brigadier General William. *Memoirs of World War I: "From Start to Finish of Our Greatest War."* New York, New York: Random House, 1960.

Nalty, Bernard C. *Winged Shield, Winged Sword: A history of the United States Air Force.* Washington, D.C.: U.S. Government Printing Office, 1997.

North Atlantic Treaty Organization (NATO). *NATO Glossary of Terms.* Brussels, Belgium: NATO Standardization Agency.

North Atlantic Treaty Organization (NATO). *NATO Handbook.* Brussels, Belgium: NATO Office of Information and Press, 2001.

"Only America Unhappy with Iran." *American Foreign Press*, Volume 2, Issue 886 (February 2005). Article on-line; available from http://www.thebangladeshtoday.com/archive/February/14-02-2005.htm; Internet; accessed 7 April 2005.

Osgood, Robert E. *Alliances and American Foreign Policy*. Baltimore, Maryland: The John Hopkins Press, 1968.

Parry, Colonel William H., III. "Multinational Operations and the National Security Strategy: The Modern Melian Dialogue." United States Army War College Strategy Research Project, 2000.

Paul, T.V., James J. Wirtz, and Michel Fortmann. *Balance of Power: Theory and Practice in the 21st Century.* Stanford, California: Stanford University Press, 2004.

Porter, Dr. Clifford F. "Asymmetrical Warfare, Transformation, and Foreign Language Capability." Combat Studies Institute Combined Arms Center Paper, April 2005.

Paper on-line; available from
http://www.leavenworth.army.mil/csi/pubs/AsymmetricalWarfare.asp; Internet;
accessed 17 April 2005.

Prior, Robin and Trevor Wilson. *Command on the Western Front*. Cambridge,
Massachusetts: Blackwell Publishers, 1992.

Rawling, Bill. *Surviving Trench Warfare: Technology and the Canadian Corps, 1914-
1918*. Toronto, Ontario: University of Toronto Press, 1992.

Realizing the Potential of C4I: Fundamental Challenges. Commission on Physical
Sciences, Mathematics, and Applications, National Research Council Committee
to Review DOD C4I Plans and Programs, 1999. Book on-line; available from
http://books.nap.edu/html/C4I/index.html; Internet; accessed 20 March 2005.

Reynish, William. "A U.S. Embarassment?" *Aviation Today* (17 March 2005). Article
on-line; available from
http://www.aviationtoday.com/cgi/av/show_mag.cgi?pub=av&mon=0902&file=0
902viewpoint.htm; Internet; accessed 17 March 2005.

Richelson, Jeffrey T. "The Calculus of Intelligence Cooperation." *International Journal
of Intelligence and Counterintelligence*, Volume 4, no. 3 (Fall 1990): 307-323.

Rothstein, Robert L. *Alliances and Small Powers*. New York, New York: Columbia
University Press, 1968.

Rumsfeld, Donald H. *The National Defense Strategy of the United States of America*.
Washington, D.C.: U.S. Government Printing Office, March 2005.

Scales, Robert H., Jr. "Trust, not technology, Sustains Coalitions." *Parameters*, Volume
XVIII, no. 4" (Winter 1998): 4-10.

Scheck, Raffael. "Germany and Europe, 1871-1945." Book on-line; available from
http://www.colby.edu/personal/r/rmscheck; Internet; accessed 23 March 2005.

Sherman, Jason. "Wolfowitz Approves Plan to Improve DoD's Foreign Language
Skills." U.S. Air Force Aim Points Inside the Pentagon Paper, March 2005.
Article on-line; available from http://aimpoints.hq.af.mil/display.cfm?id=1768;
Internet; accessed 3 April 2005.

Shulsky, Abram N. and Gary J. Schmitt. *Silent Warfare: Understanding the World of
Intelligence*, 3rd ed. Washington, D.C.: Brassey's Inc., 2002.

Soanes, Catherine. *Pocket Oxford English Dictionary*. 9th ed. Oxford, New York:
Oxford University Press, Inc., 2002.

Sokolsky, Richard, Stuart Johnson, and F. Stephen Larrabee. *Improving Allied Military Contributions*. Arlington, Virginia: Rand Corporation, 2000.

Spartacus Schoolnet. "Wireless Communications." http://www.spartacus.schoolnet.co.uk/FWWwireless.htm; Internet; accessed 6 February 2005.

Spring, S.C., Dennis M. Gormley, K. Scott McMahon, Kenneth Smith, and Daniel Hobbes. *Information Sharing for Dynamic Coalitions*. Report prepared for the Air Force Research Laboratory. Arlington, Virginia: Pacific Sierra Research, December 2000.

Statement of Linton Wells II Acting Secretary of Defense for Networks and Information Integration and DoD Chief Information Officer Before The House Armed Services Committee, Terrorism, Unconventional Threats and Capabilities Subcommittee. House Committee on Armed Services, March 2005.

Steele, Robert David. *On Intelligence: Spies and Secrecy in an Open World*. Fairfax, Virginia: AFCEA International Press, May 2000.

Storr, Lieutenant Colonel J.P. PhD. *The Command of British Land Forces in Iraq, March to May 2003* (2003). Report on-line; available from http://www.dodccrp.org/events/2004/ICCRTS_Denmark/CD/papers/068.pdf; Internet; accessed 16 April 2005.

Peter B. Teets. *Regarding the Fiscal Year 2005 National Defense Authorization Budget Request: Status of the Space Programs*. House Armed Services Committee Statement by the Undersecretary of the Air Force, February 2004. Statement on-line; available from http://armedservices.house.gov/openingstatementsandpressreleases/108thcongress/04-02-25teets.html; Internet; accessed 15 March 2005.

Temin, Thomas. "DoD to shelve GCCS, Roll Out New System." Government Computer News (26 April 2004). Article on-line; available from http://www.gcn.com/23_9/news/25684-1.html; Internet; accessed 14 March 2005.

Tiboni, Frank and Matthew French. "Blue Force Tracking Gains Ground." Federal Computer Weekly (22 March 2004). Article on-line; available from http://www.fcw.com/fcw/articles/2004/0322/tec-blueforce-03-22-04.asp; Internet; accessed 17 March 2005.

Tzu, Sun. *Sun Tzu: The New Translation*. Edited and translated J.H. Huang andC.J. Phillips. New York, New York: William Morrow and Company, Inc., 1993.

United Nations. *UNTERM database*. http://unterm.un.org/; Internet; accessed 19 March 2005.

United States. "A Brief History of Basic Intelligence and The World Factbook." *Central Intelligence Agency: The World Factbook* (December 2004). Article on-line; available from http://www.odci.gov/cia/publications/factbook/docs/history.html; Internet; accessed 14 April 2005.

United States. Air Force Press Network (AFPN). "Airborne Network to Link Sensors, Shooters, Decision Makers." *Intercom*, Volume 46, No. 4 (April 2005): 19.

United States, Committee to Review DOD C4I Plans and Programs, Commission on Physical Sciences, Mathematics, and Applications, National Research Council, *Realizing the Potential of C4I: Fundamental Challenges* (Washington, D.C.: National Academy of Sciences, 1999) [book on-line]; available from http://books.nap.edu/html/C4I/index.html; Internet; accessed 20 March 2005.

United States. Defense Acquisition University. "Defense Acquisition Guidebook," http://akss.dau.mil/dag/; Internet; accessed 13 March 2005.

United States. Defense Information Systems Agency (DISA). "Global Combat Support System (GCSS) Combatant Commanders/ Joint Task Force (CC/JTF)." DISA Website (January 2005). Article on-line; available from http://www.disa.mil/main/prodsol/gcss.html; Internet; accessed 17 March 2005.

United States. Defense Information Systems Agency (DISA). "Joint Command and Control (JC2)." http://www.les.disa.mil/c/extranet/home?e_l_id=33; Internet; accessed 14 March 2005.

United States. Defense Information Systems Agency (DISA). "Joint Command and Control (JC2)." *DISA Fact Sheets* (December 2004). Fact sheet on-line; available from http://www.disa.mil/pao/fs/jc2_3.html; Internet; accessed 19 April 2005.

United States. Defense Systems Management College (DMSC). *Glossary: Defense Acquisition Acronyms and Terms*, 6th Ed. Fort Belvoir, Virginia: DMSC Press, March 1995.

United States. Department of Defense. *Coalition Theater Logistics Advanced Concept Technology Demonstaration (CTL-ACTD) Management Plan*. Washington, D.C.: U.S. Government Printing Office, November 2001.

United States. Department of Defense. *Defense Language Transformation Roadmap.* Washington, D.C.: U.S. Government Printing Office, June 2004.

United States. Department of Defense. *Department of Defense Instruction, No. 8110.1*: *Multinational Information Sharing Networks Implementation*. Washington, D.C.: U.S. Government Printing Office, February 2004.

United States. Department of Defense. *Department of Defense Directive Number 8100.1: Global Information Grid Overarching Policy*. Washington, D.C.: U.S. Government Printing Office, 2003.

United States. Department of Defense. *Network Centric Environment Joint Functional Concept*. Washington, D.C.: U.S. Government Printing Office, November 2004.

United States. Director National Security Agency. *Multinational Information Sharing (MNIS) Protection Profile (PP) For Networked Information Systems*. Fort Meade Maryland: U.S. Government Printing Office, September 2002.

United States. Director of Central Intelligence. "Iraq's Continuing Programs for Weapons of Mass Destruction." National Intelligence Estimate, NIE 2002-16HC. Washington, D.C.: Central Intelligence Agency, April 2004.

United States. *The Intelligence Community of the 21st Century*. One Hundred Fourth Congress House of Representatives Staff Study, (June 1996). Study on-line; available from http://www.au.af.mil/au/awc/awcgate/congress/ic21/ic21_toc.html; Internet; accessed 2 April 2005.

United States. Government Accountability Office. *The Global Information Grid and Challenges Facing Its Implementation*. House of Representatives Subcommittee on Terrorism, Unconventional Threats, and Capabilities, Committee on Armed Services Report. Washington, D.C.: U.S. Government Printing Office, July 2004.

United States. Joint Chiefs of Staff. *Joint Publication 2-01: Joint and National Intelligence Support to Military Operations*. Washington, D.C.: U.S. Government Printing Office, October 2004.

United States. Joint Chiefs of Staff. *Joint Publication 3-0: Doctrine for Joint Operations*. Washington, D.C.: U.S. Government Printing Office, September 2001.

United States. Joint Chiefs of Staff. *Joint Publication3-13: Joint Doctrine for Information Operations*. Washington, D.C.: U.S. Government Printing Office, October 1998.

United States. Joint Chiefs of Staff. *Joint Publication 3-16: Joint Doctrine for Multinational Operations*. Washington, D.C.: U.S. Government Printing Office, February 1999.

United States, Joint Chiefs of Staff, *Joint Publication 6-0: Doctrine for Command, Control, Communications, and Computers (C4) System Support in Joint Operations* (Washington, D.C.: U.S. Government Printing Office, May 1995), II-9.

United States. Joint Chiefs of Staff. *Joint Vision 2020.* Washington, D.C.: U.S. Government Printing Office, December 2000.

United States. Joint Requirements Oversight Council. *Joint Tactical Radio System (JTRS) Operational Requirements Document (ORD)*, Version 3.2. Washington, D.C.: U.S. Government Printing Office, April 2003.

United States. The Joint Warfare Center. *Joint Doctrine Series Pamphlet 5: Operational Implications of the Collaborative Information Environment (CIE).* Washington, D.C.: U.S. Government Printing Office, June 2004.

United States. National Security Agency. *Operations Security: Intelligence Threat Handbook*. Greenbelt, Maryland: The Interagency Support Staff, May 1996.

United States. Secretary of the Air Force. *Air Force Doctrine Document 2-4: Combat Support.* Washington, D.C.: U.S. Government Printing Office, November 1999.

United States. Secretary of the Army. *Army Digitization Master Plan '96.* Washington, D.C.: U.S. Government Printing Office, 1996. Article on-line; available from http://www.globalsecurity.org/military/library/report/1996/army_digit_m-plan96.htm; Internet; accessed 10 April 2005.

United States. Secretary of the Army. "Army Regulation 530-1 OPSEC, Appendix D: The Hostile Intelligence Threat" (1985).   Regulation on-line; available from http://www.fas.org/irp/doddir/army/ar530-1d.htm; Internet; accessed 5 April 2005.

United States. Secretary of the Army. *Field Manual 34-2: Collection Management and Synchronization Planning.* Washington, D.C.: U.S. Government Printing Office, 1994.

United States. Secretary of the Army. *Field Manual 100-7: Decisive Force: The Army in Theater Operations*. Washington, D.C.: U.S. Government Printing Office, 1995.

United States. Secretary of the Army. *Field Manual 100-8: The Army in Multinational Operations*. Washington, D.C.: U.S. Government Printing Office, February 1999.

United States. The White House. *The National Strategy of the United States of America.* Washington, D.C.: U.S. Government Printing Office, September 2002.

United States. The White House. The National Security Strategy of the United States of America. Washington, D.C.: U. S. Government Printing Office, 2005.

Wagner, Lieutenant General Robert W. *C4 Systems and the Role of U.S. Joint Forces Command in Developing a "Coherently Integrated Joint Force."* House of Representatives House Armed Service Committee Subcommittee Terrorism, Unconventional Threats and Capabilities Statement, March 2005.

Wagner, Lieutenant General Robert W. *C4 Systems and the Role of U.S. Joint Forces Command in Developing a "Coherently Integrated Joint Force."* Statement Before the Subcommittee Terrorism, Unconventional Threats and Capabilities, House Armed Service Committee, U.S. House of Representatives. Washington, D.C.: United States Congress, March 2005.

Wall, Captain Steven T. "Joint Tactical Radio System: Volume, Distance and Speed." *Field Artillery Journal*, HQDA PB 6-00-1. Fort Sill, Oklahoma: U.S. Field Artillery Association, January-February 2000.

Waltz, Edward. *Knowledge Management in the Intelligence Enterprise.* Boston, Massachusetts: Artech House Inc., 2003.

Wegner, Captain Neal J. "The Intel XXI Concept III: The Seven Intelligence Tasks." *Military Intelligence Professional Bulletin* (January – March 1997). Article on-line; available from http://www.fas.org/irp/agency/army/tradoc/usaic/mipb/1997-1/cncp9701.htm; Internet; accessed 18 April 2005.

Williams, Commander Charles A. "Intelligence Support to U.N. Peacekeeping Operations." Washington, D.C.: National Defense University Industrial College of the Armed Forces Paper, 1993.

Wilson, Clay. *Network Centric Warfare: Background and Oversight Issues for Congress.* CRS Report for Congress. Washington, D.C.: The Library of Congress, Technology and National Security Foreign Affairs, Defense, and Trade Division.

Wikipedia. "World War I." http://en.wikipedia.org/wiki/World_War_I; Internet; accessed 5 February 2005.

Wirtz, James J. "Constraints on Intelligence Collaboration: The Domestic Dimension." *International Journal of Intelligence and Counterintelligence,* Volume 6 no.1 (Spring 1993): 85-99.

WordiQ.com. "Auld Alliance." http://www.wordiq.com/definition/Auld_Alliance.html; Internet; accessed 26 March 2005.