Intelligence Collection:

Supporting Full Spectrum Dominance and Network Centric Warfare?

A Monograph
by
Major Bruce D. Moses
United States Army

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas
AY 03-04

SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

Major Bruce D. Moses

Title of Monograph: Intelligence Collection: Supporting Full Spectrum Dominance and Network Centric Warfare?

Approved by:

_____	**Monograph Director**
COL Bruce J. Reider, MMAS	
_____	**Professor and Director Academic Affairs, School of Advanced Military Studies**
COL Kevin C. M. Benson, MMAS	
_____	**Director, Graduate Degree Program**
Robert F. Baumann, Ph.D.	

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	26 March, 2004	Monograph

4. TITLE AND SUBTITLE
Intelligence Collection: Supporting Full Spectrum Dominance and Network Centric Warfare?

5. FUNDING NUMBERS

6. AUTHOR(S)
Major Bruce D. Moses

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

U.S. Army Command and General Staff College
School of Advanced Military Studies
250 Gibbon Ave.
Fort Leavenworth, KS 66027

8. PERFORMING ORGANIZATION REPORT NUMBER

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

U.S. Army Command and General Staff College
Fort Leavenworth, KS 66027

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

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

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

This monograph examines whether the Army's information collection efforts are supporting the goal of full spectrum dominance and whether these are in harmony with the concepts of network centric warfare. Full spectrum dominance and network centric warfare are central themes in Department of Defense and Army transformation literature and both require information collection and an understanding of the role of cognition empowered by networking for success. More specifically, it examines whether Army collection efforts are focusing too heavily on collection for combat operations and leaving it unable to fully exploit the access to adversary systems during stability operations.

This study found that the institutional Army is not fully supporting the goal of full spectrum dominance or network centric warfare but is still myopically investing heavily in efforts to defeat the adversary's conventional capabilities with standoff collection technology and is not creating the organizational, systems and technical architectures necessary to leverage the power of a fully networked force.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Intelligence, Network Centric Warfare, Full Spectrum Dominance	78
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
U	U	U	none

Abstract

Intelligence Collection: Supporting Full Spectrum Dominance and Network Centric Warfare? By Major Bruce D. Moses, United States Army, 78 pages.

This monograph examines whether the Army's information collection efforts are supporting the goal of full spectrum dominance and whether these are in harmony with the concepts of network centric warfare. Full spectrum dominance and network centric warfare are central themes in Department of Defense and Army transformation literature and both require information collection and an understanding of the role of cognition empowered by networking for success. More specifically, it examines whether Army collection efforts are focusing too heavily on collection for combat operations and leaving it unable to fully exploit the access to adversary systems during stability operations (such as the occupation of another nation). It examines the theory and doctrine behind these two transformation objectives and compares this with the current capabilities and efforts.

This study consisted of four major efforts. First, it examined theory and doctrine to develop the methodology and criteria for this study. Second, it examined the physical domain and history of collection systems to establish a basic understanding of the capabilities and limitations of collection platforms and sensors. Third, it examined the relationships of these systems in the context of full spectrum operations to see how relationships and capabilities change over time. Fourth, it then analyzed how well the Army's information collection efforts are supporting the goal of full spectrum dominance and if they are in harmony with network centric warfare.

This study found that the institutional Army is not fully supporting the goal of full spectrum dominance but is still myopically investing heavily in efforts to defeat the adversary's conventional capabilities with standoff technology. This indicates that the Army still does not accept its dual role as a controlling force as well as a fighting force. This study also found that the institutional Army is also not fully supporting network centric warfare. The Army is still investing heavily in trying to conduct fusion of raw data forward in expensive shelters and closed networks that connect through very low bandwidth dissemination pipes to everyone else. This effort ignores the role of cognition in converting information into intelligence and the power of networking in a high bandwidth environment. In simple terms, network centric warfare is all about accelerating the speed of information and maximizing human connectivity (leveraging the power of the human mind) not replacing it with machines. The most important finding of all is the lack of investment in training and educating soldiers. The Army has moved away from training people to make informed decisions about information through leveraging technology toward training people to feed machines that support targeting. This can work in standoff precision warfare but it will not work in a close fight or in stability operations.

TABLE OF CONTENTS

List of Figures

Introduction

The Chief of Staff of the U.S. Army, General Schoomaker, is trying to "accelerate the Future Force network to enhance the Joint Battle Command capabilities of the Current Force".[1] The U.S. Department of Defense (DOD) is pursuing a transformation vision toward a military that is empowered by a network centric architecture. The executive summary in a DOD report to Congress on network centric warfare begins by stating, "Network Centric Warfare represents a powerful set of warfighting concepts and associated military capabilities that allow warfighters to take full advantage of all available information and bring all available assets to bear in a rapid and flexible manner."[2]

The aim of these efforts is information superiority and knowledge dominance over an adversary enabled through digital networking. The unifying concept is a single interoperable global network that provides joint, interagency, and multinational partners' unfettered access to actionable knowledge. The resulting common situational awareness enables them to conduct rapid, decisive and synergistic effects based operations faster than the adversary can react. [3] According to Robert Leonard, "both knowledge and ignorance have dominated warfare throughout history, but Information Age warfare has adjusted the balance toward knowledge".[4]

However, networks only use *available* information. Networks do not collect information in the physical domain in which a land force operates. The land force operates in jungles, cities, and mountains. In these environments physics, a thinking enemy, and economics (scarcity of funding) all conspire against the land force ever having enough collection assets, connectivity or

---

1 Peter J. Schoomaker, Gen, CSA. The Way Ahead: Our Army at War ... Relevant and Ready. Moving from the Current Force to the Future Force …Now! (Washington, DC: Army Strategic Communications, November 2003), 11.

2 U.S. Department of Defense, Network Centric Warfare Department of Defense Report to Congress [document on-line] (Washington, DC: Government Printing Office, July 2001, accessed 24 October 2003); available from http://www.dod.mil/nii/ncw; Internet.

3 Edward A. Smith, Effects Based Operations: Applying Network Centric Warfare in Peace, Crisis, and War (Vienna, VA: CCRP, 2002), xiv.

4 Robert R. Leonard, The Principles of War for the Information Age (New York, NY: Ballantine Books, 1998), 252.

unlimited bandwidth to achieve perfect knowledge at all times in every situation. Even with all the advances in collection, information sharing and understanding these will not eliminate or overcome the fog and friction of war.[5] Time is major factor in preventing perfect awareness. Leonard argues, "Conflict is time competitive, he [a commander] must choose not to know certain aspects, and he must adapt his activity to most efficiently manage that ignorance".[6]

Conflict is also a very human endeavor. Technology is great for processing and transporting information. Nevertheless, it does not work well without information. Gary Klein points out in his research on decision making that the human mind can replace ignorance with deductive logical thinking, analysis of probabilities, and statistical methods. Computers can greatly assists in these processes and help fill in the holes. However, decision makers in a field setting will always operate in a fog of ignorance to some extent. They do not have the luxury of time to conduct detailed analysis. Instead, Klein found that he or she relies on very human processes of intuition, mental stimulation, metaphor and storytelling to make decisions.[7]

Converting information into intelligence involves human decisions at every step.[8] The closer the adversary is the more human and more time competitive this process is. While technology can replace mechanical processes and assist in visualization of information, it will not replace decision-making in the near future. Managing scarce resources, deciding what to collect, when to collect it, what is significant to report, what is not, the analysis of enemy intentions, how to present intelligence products are all human decisions. Until artificial intelligence becomes reality and we are then willing to trust our lives to it, the automatic fusion and decision-making by computers alone is at present not realistic.

---

5 Jacob W. Kipp and Lester W. Grau, "The Fog and Friction of Technology," Military Review LXXXI, no. 5 (September-October 2001), 97.

6 Robert R. Leonard, The Principles of War for the Information Age, (New York, NY: Ballantine Books, 1998), 252.

7 Gary Klein, Sources of Power: How People Make Decisions, (Cambridge, MA: The MIT Press, 1998), 3.

8 U.S. Department of Defense, Joint Publication (JP) 1-02: Department of Defense Dictionary of Military and Associated Terms, (Washington, D.C.: US Government Printing Office, 2000), 262. This is the definition of the DOD Intelligence Cycle.

This monograph examines whether the Army's information collection efforts are supporting the goal of full spectrum dominance and whether these are in harmony with the concepts of network centric warfare. Full spectrum dominance and network centric warfare are central themes in transformation literature and both require information collection for success.

Methodology

> The Joint Operations Concepts (JOpsC) describe how the Joint Force intends to operate 15-20 years in the future across the full range of operations. …The JOpsC builds on the goal of Full Spectrum Dominance: the defeat of any adversary or control of any situation across the full range of military operations. Full Spectrum Dominance is based on the ability to sense, understand, decide, and act faster than an adversary in any situation.
>
> General Peter J. Schoomaker[9]

In this study, the goal of full spectrum dominance framed the methodology for examining the research question. The focus of the analysis was on the Army's roles and ability to collect during combat and stability operations in support of a joint force. The collection requirements of these two operations represent vastly different collection challenges and provide sufficient context to answer the research question. Recent operations in Iraq (or for that matter Vietnam, World War II …) highlight that both can occur simultaneously within the same battlespace.

According to General Schoomaker, "Full Spectrum Dominance is based on the ability to *sense*, *understand*, *decide* and *act faster* than an adversary in any situation."[10] In this sentence, he establishes the relationship between three of the four domains of information warfare: The physical domain where collection occurs, the information domain where manipulation of information occurs and the cognitive domain where the human mind makes decisions about information.[11]

---

9 Schoomaker, 5.

10 Ibid,. 5.

11 David S. Alberts et al., Understanding Information Age Warfare, (Vienna, VA: CCRP, 2001), 12-13. The fourth is the social domain, which focuses with interactions of people on a network. This study will not dig into the cultural or psychological aspects of information management

Sensing occurs in the physical domain where the collection and transmission of information about the adversary occurs. This includes collecting and updating information on friendly and neutral elements. [12] It also includes all the equipment, organizations, and frequencies that facilitate the transport of information to those who produce knowledge (or greater understanding) and the delivery of products to decision makers. [13]

Understanding and deciding occur in the cognitive domain of the human mind. The Army often refers to this as the art of command or "battle command". *FM 3.0, Operations* defines battle command as "the exercise of command in operations against a hostile, thinking enemy. Skilled judgment gained from practice, reflection, study, experience, and intuition often guides it."[14] Cognition is also an integral part of information collection. A human mind is required to plan and direct collection efforts, interpret collection, decide what to report, and conduct analysis.

Intelligence estimates are also the products of cognition that in turn support a commander's cognitive battle command process. According to *FM 3.0, Operations*, "Effective battle command demands decisions that are both timely and more effective than those of the enemy. Success often depends on superior information that enables superior decisions."[15] Manuel De Landa argues that "[artificial intelligence] technologies are still in their infancy, and so human analysts are not threatened yet to be taken out of the decision-making process". [16] Computers are getting better at speeding up mechanical processing and displaying things through pattern recognition. However, the human mind is still required to verify these efforts, look for additional information in the collection, detect deception efforts and convert all the information into products that facilitates understanding.

---

12 Friendly force information elements include things like size, activity, location, unit, equipment, boundaries … Neutral elements include things like terrain and weather.

13 Alberts, Understanding Information Age Warfare, 12.

14 U.S. Department of the Army, FM 3-0: Operations, (Washington, D.C.: US Government Printing Office, 2001), 5-1.

15 Ibid., 5-2.

16 Manuel De Landa, War in the Age of Intelligent Machines, (New York, NY; Urzone Inc., 1991), 181.

The ability to "*act faster*" is what the information domain (network centric warfare) promises to provide. A network-centric concept of warfighting, according to Alberts, "is focused upon sharing and collaboration to create increased awareness, shared awareness, enabling collaboration, and, as a result, improved synchronization".[17] Networking in a robust interoperable and high bandwidth environment accelerates cognitive processes through information velocity. This in turn increases the speed of understanding, decision-making and the application of effects.

Development of Evaluation Criteria

Army collection systems are part of a non-linear system-of-systems architecture. Full spectrum dominance and network centric warfare are also non-linear concepts. Instead of taking things apart and applying standard evaluation criteria, we will use a systems approach to these systems. Interdependence is fundamental to both full spectrum dominance and network centric warfare. Jasmshid Gharajedaghi in his work, *Systems Thinking: Managing Chaos and Complexity*, provides a simple explanation of the difference between traditional analysis and systems thinking:

Understanding interdependency requires a way of thinking different from analysis; it requires systems thinking. And analytical thinking and systems thinking are quite distinct. Analysis is a three-step thought process. First, it takes apart that which it seeks to understand. Then it attempts to explain the behavior of the parts taken separately. Finally, it tries to aggregate understanding of the parts into an explanation of the whole. Systems thinking uses a different process. It puts the system in the context of the larger environment of which it is a part and studies the role it plays in the larger whole. (Gharajedaghi 1999, 15)

17 Alberts, Understanding Information Age Warfare, 71.

With this description in mind, this will guide the development of the evaluation criteria. Full spectrum dominance involves two broad objectives: defeat and control. Defeat in this context involves those collection activities that primarily focus on the destruction of the armed forces. These are traditionally associated with combat operations. Control involves collection activities that generally focus on preventing the adversary from rising up from defeat (or rendering it incapable of resisting our will). This traditionally involves collection activities typically associated with stability operations. Along with information operations,[18] which tie both together, these work toward the common aim of overcoming the enemy's will.[19]

The DOD intelligence cycle and the literature on network centric warfare provide the means to develop the systems criterion for evaluating the Army collection effort within the larger system-of-systems architecture. The DOD Intelligence Cycle provides the means to separate the modular components of each system into the three domains of information warfare. The literature on network centric warfare provides the means to conduct an end-to-end analysis of the individual system architectures and see how it works within the larger architecture.

The DOD Intelligence Cycle

According to *Joint Publication (JP) 2-0, Doctrine for Intelligence Support to Joint Operations*, the intelligence cycle is the "process by which information is converted into intelligence and made available to users".[20] This cycle "establishes the basis for common joint intelligence terminology, tactics, techniques, and procedures" and consists of six phases: Planning

18 Information operations are defined in Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms (254) as those "actions taken to affect adversary information and information systems while defending one's own information and information systems.

19 Theorists will recognize the influence of Carl Von Clausewitz in the framework of this concept as shown in Clausewitz, Carl Von, On War. Edited and translated by Michael Howard and Peter Paret. (New York, NY: Everyman's Library, 1993), 102. In a later chapter of On War, he also addresses intelligence in war. While he recognized intelligence as the basis for plans and operations, he had a low regard for collection. "Many intelligence reports in war are contradictory; even more are false, and most are uncertain" (136). The difficulty this creates for decision makers "constitutes one of the most serious sources of friction in war" and the creator of more fog (137). In On War (117), he holds military genius in high regard. One of it major elements is the cognitive ability to "scent out the truth" from this fog. This danger still exists. It is important to post information to a network for common situational awareness. However, this collection requires trained personnel who report facts without interpretation. Most importantly, the analysis requires professionals who can 'scent out the truth' and not create fog. This is important whether the commander does it or an intelligence specialist assists him or her in this effort.

20 Joint Publication (JP) 1-02: Department of Defense Dictionary of Military and Associated Terms, 262.

and Direction, Collection, Processing and Exploitation, Analysis and Production, Dissemination and Integration. [21] In the descriptions that follow, note the heavy role cognitive functions play in every phase of this cycle.

The *planning and direction* phase is a cognitive function performed by collection managers based on the commander's priority intelligence requirements. This step is required due to a scarcity of collection systems, limited connectivity and limited bandwidth. Scarcity requires planning and direction to focus efforts. According to Leonard, "Information leads to precise expenditure of resources, and therefore to economy. Indeed, the entire purpose of intelligence in warfare is to economize – to inform our efforts in order to gain effect at the least cost."[22]

The *collection* phase is a physical activity performed by a variety of means from soldiers to satellites. According to Melton, this is "the second oldest profession".[23] Throughout history, intelligence has played a role, for good or ill, in the victory and defeat of armies and nations. [24] John Keegan, a noted historian, found that "The Bible contains more than a hundred references to spies and intelligence-gathering."[25] Many have paid with their lives in an attempt to collect information and our nation spends billions to collect and protect it.

The *processing and exploitation* phase involves the conversion of information into forms that enable analysis. This is usually a digital form. This includes initial imagery interpretation, document translation, translating foreign languages, converting raw electronic intelligence into standard message formats. This requires human cognition to perform this process or at least verify the process. The focus is on putting facts into the system not performing analysis itself. However, specialized intelligence collection often requires analysis at this step. [26]

---

21 U.S. Department of Defense, Joint Publication (JP) 2-0: Doctrine for Intelligence Support to Joint Operations (Washington, D.C.: US Government Printing Office, 2000), II-1.

22 Leonard, 219.

23 H. Keith Melton, The Ultimate Spy Book (New York, NY: DK Publishing, 1996), 7.

24 John Keegan, Intelligence in War: Knowledge of the Enemy From Napoleon to Al-Queda (New York, NY: Random House, 2003), 7-17.

25 Ibid., 18.

26 Joint Publication (JP) 2-0: Doctrine for Intelligence Support to Joint Operations, II-7.

The *analysis and production* phase is another cognitive effort where according to *JP 2-0: Doctrine for Intelligence Support to Joint Operations*, "all available processed information is integrated, analyzed, evaluated, and interpreted to create products … They may be oral presentations, hard copy publications, or electronic media."[27] Some mistake information management with intelligence. Imagery, electronic signals, databases and other forms of information compiled in a computer is not intelligence. These are artifacts. Even the manipulation of this data on a computer display is not intelligence.

Intelligence is a human decision about the adversary's information. It is not until an analyst[28] applies some meaning to these to produce understanding or knowledge is it intelligence. It is particularly important to comprehend the enemy point of view in all aspects.[29] This requires detailed knowledge about the adversary. Someone with a great deal of knowledge and time observing the adversary will see the data differently from someone who just pulls it up on the computer screen. Those who make judgments about information on the adversary are performing intelligence. Those who decide what to collect or report about the adversary are also performing an intelligence function. Therefore, everyone who has anything to do with the adversary or his environment and makes a decision such as what to report is performing an intelligence function.

The *dissemination and integration* phase is in both the physical and information domains. Information must physically move from one point to another but it also must be in a form that is appropriate for the person receiving it. A soldier who is at the farthest reaches of a network (low bandwidth environment) does not have time to wait for some huge imagery file to pass from one end of the tactical internet to the other. Intelligence production must recognize that the ultimate consumer is the soldier not another intelligence organization. According to Keegan, "Knowledge, the conventional wisdom has it, is power; but knowledge cannot destroy or deflect damage or

---

27 Ibid., II-8.

28 When a commander makes a decision about information, they are the intelligence analyst.

29 Abram N. Shulsky and Gary J. Schmitt, Silent Warfare: Understanding the World of Intelligence, Third Edition, (Washington, D.C.:Brassey's Inc., 2002), 54.

even defy an offensive initiative by an enemy unless the possession of knowledge is allied to objective force."[30] Time, from collection to delivery to those who can act on it is critical.

The *evaluation and feedback* phase occurs throughout the process. It is a constant human evaluation of the whether the intelligence is timely, accurate, usable, complete, relevant, objective and available.[31] The environment is not static. Battlespace geometry changes as the air, sea, and land forces move into once denied areas. Therefore, planning and direction of intelligence collection is dynamic as well. The enemy also has a vote. It can disperse, hide, deceive, deny and defeat collection efforts. The weather and terrain can also play a role in collection, connectivity, and dissemination of products. It is important to understand the human processes at each stage in converting information into intelligence when developing organizational, systems and technical architectures for network centric warfare.

Network Centric Warfare

According to Alberts, "Network Centric Warfare (NCW) translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace."[32] It does this through a robust interoperable network called the global information grid. According to the *Capstone Requirement Document (CRD) for the Global Information Grid (GIG)*, the GIG is a "globally interconnected, 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. The GIG supports all DoD, National Security, and related Intelligence Community (IC) missions and functions (strategic, operational, tactical, and business) in war and in peace." [33] At its core is a robust fiber backbone

---

30 John Keegan, Intelligence in War: Knowledge of the Enemy from Napoleon to Al-Queda (New York, NY: Alfred A. Knopf), 348.

31 Ibid., II-14.

32 David S. Alberts, John J. Garstka, Fredrick P. Stein. Network Centric Warfare: Developing and Leveraging Information Superiority, 2nd Edition (Revised), (Vienna, VA: CCRP, 1999), 2.

33 Commander in Chief, Joint Forces Command, Capstone Requirement Document (CRD) for the Global Information Grid (GIG). [document on-line] (Washington, DC: Government Printing Office, March 2001, accessed 27 November 2003, available from http://www.dfas.mil/technology/pal/regs/gigcrdflaglevel review.pdf; Internet, 2.

that creates an environment where bandwidth is essentially unconstrained between nodes (knowledge centers). It creates the ability to transport and process information with maximum velocity enabling the acceleration of informed decision-making.[34]

This fiber backbone also links to every form of communication (military and commercial) enabling redundant means to disseminate products to consumers through dedicated point-to-point communications, wideband broadcasts, and narrow band broadcasts. Once a land force gains access to the adversary's communication infrastructure, it can also leverage it as well. Communication from this fiber grid is more robust and capable of communicating to elements on the battlefield than battlefield elements can communicate with each other through the tactical internet. In this architecture, the low bandwidth tactical internet is a command and control circuit that controls the high bandwidth information circuit and dissemination system.

According to Brower, "The Global Information Grid Architecture is the Department of Defense's enterprise architecture that will break down the communications, interoperability and security barriers to information dominance … a quantum leap in network centric capabilities."[35] This assumes the Army is changing its organizational, systems and technical architectures to leverage this power. The GIG does not fix the bandwidth problem in the forward areas. Instead, it provides the ability to work around it to improve collection support to commanders.

According to Alberts, "It [network centric warfare] requires concepts of operation, C2 approaches, organizational forms, doctrine, force structure, support services and the like – all working together to leverage the available information".[36] To leverage the power of network centric warfare requires those elements involved with processing, exploitation, analysis and production of information to be inside the high bandwidth environment. It is not enough to

---

34 LTC Charles Harvey and LTC Lance Schultz, "An Analysis of the Impact of Network-Centric Warfare on the Doctrine and Tactics, Techniques and Procedures of Intelligence at the Operational Level," Naval War College Paper, (1 June 1999), 14.

35 J. Michael Brower, "Bandwidth Bonanza," Military Information Technology, Volume 7, Issue 10 (December 2003/January 2004): 20-21.

36 Ibid., 3.

connect to it. Network centric warfare requires arranging the modular components of each collection system into configurations that maximize the power of the global information grid.

One myth of network centric warfare is that it replaces people with technology. After looking at the DOD intelligence cycle, we know that cognitive decisions are involved at every step from collecting information to converting information into intelligence and in product development. Replacing people in this process, or not investing in their training, is a dangerous idea. The quality of personnel at each step and how well informed they are determines whether the products they generate create greater understanding or greater fog and friction. The power of network centric warfare is informing decision makers faster not replacing people with computers.

In the high bandwidth portion of the GIG, there is theoretically no limit to what an analyst can leverage. Those inside this environment receive information in near real time from more sources and in volumes not possible in the tactical environment. Those outside this environment (i.e. in a Tactical Exploitation System) where the bandwidth is restricted cannot leverage a fraction of this power.[37] However, those in forward areas have more current information about the local environment than those on the GIG. They become a source of informed knowledge for everyone else.

What the GIG enables is the ability to change the location of people, processes and quality of the decisions. People are empowered not replaced. The three basic tenets of network centric warfare according to Alberts are, "[1] A robustly networked force improves information sharing. [2] Information sharing and collaboration enhances the quality of information and shared situational awareness. [3] Shared situational awareness enables collaboration and self-synchronization. These in turn, dramatically increase mission effectiveness."[38] What the GIG enables is a change to the Army's organizational, systems and technical architectures. It offers the

37 Those in the high bandwidth portion of the GIG can search years of imagery files and query thousands of servers across the GIG in near real time. However, the analysts up forward have access to current intelligence and can make better decisions about the current situation. The power of Network Centric Warfare is about networking between people and systems not replacing the altogether.

38 David S. Alberts, Richard E. Hayes, Power to the Edge: Command… Control… in the Information Age (Vienna, VA: CCRP, 2003), 108.

opportunity to reduce hardware pushed forward tethered to small communications pipes and move decision makers about information back to an environment where they are better informed.

The high bandwidth portion of the GIG enables more humans and machines to work together faster and produce better products in support of those who take action. This essentially unconstrained bandwidth environment provides access to all information, knowledge and experts anywhere on the GIG. The intelligence cycle is all about making informed decisions about information at every step along the way. The difference between creating fog and knowledge are the individuals making these decisions. Having these people resident on the GIG, enables the mobilization of information among those who can make the most informed decisions about it.

Currently, we are sending raw data forward into a low bandwidth environment where there is scarcity of every resource (processing, workstations, and analysts) and limited ability to disseminate information horizontally. We are then mobilizing people to that environment to make decisions about the information instead of in an unconstrained environment. There is no reason to mobilize people forward to make less informed decisions about information. Those analysts forward need to focus on the collection and analysis of local information and inform those on the GIG (common operation picture and intelligence). Those on the GIG in turn focus collection to serve the local commander better. A reserve unit could work from their hometown instead of mobilizing to a foreign country or austere environment to do the same tasks. If the human skills are not resident somewhere on the high bandwidth portion of the GIG, a node (knowledge center) on the GIG can expand to meet this requirement.[39]

39 Some question the vulnerability of the information architecture. The high bandwidth portion of the GIG will have redundancy and the information is stored across it and backed up at different locations. It is a self-healing network since another knowledge center can pick up the mission or reroute information. However, the Army does have a problem with not having an airborne retransmission platform of satellite broadcasts or the ability to communicate between elements within the same organizations. Satellites require line-of-sight and are low power, which makes them vulnerable to jamming.

Evaluation Criteria

From the examination of theory and doctrine, we now have the means to develop the criterion (or tests) to answer the research question. The two systems evaluation criteria we will use are as follows: First, full spectrum dominance requires collection systems that support both the defeat of the adversary's fighting forces in combat and control of the adversary in stability operations. Together these support information operations. The Army does not perform any of these on its own but as part of a joint team. The next two chapters will narrow down the Army's capabilities and roles and the third provides analysis of the Army's effort in supporting this goal.

Second, network centric warfare requires arranging the modular components of each collection system into configurations that maximize the power of the GIG. There are three basic components to this. Place as many of those elements of a collection system involved with processing, exploitation, analysis and production inside the high bandwidth environment of the GIG as possible. The collection system must to post information to the GIG as fast as possible (this supports building the Common Operating Picture, the intelligence cycle and dissemination). The most important requirement is the training of personnel at every step in the process (how to collect information, leverage knowledge and make decisions about information…) to support collection in both combat and stability operations.

This study consisted of four major efforts. First, we examined theory and doctrine to develop the methodology and criteria for this study. Second, we examined the physical domain and history of collection systems to establish a basic understanding of the capabilities and limitations of collection platforms and sensors. Third, we examined the relationships of these systems in the context of full spectrum operations (all three domains) to see how relationships and capabilities change over time. Fourth, we then analyzed how well the Army's information collection efforts are supporting the goal of full spectrum dominance and if they are in harmony with the concepts of network centric warfare.

Conclusion

This study found that the institutional Army is not fully supporting the goal of full spectrum dominance but is still myopically investing heavily in efforts to defeat the adversary's conventional capabilities with standoff technology. This indicates that the Army still does not accept its role as a controlling force as well as a fighting force. However, there are indicators that the operational Army is learning the importance of close access collection in stability operations.

This study also found that the institutional Army is also not investing in network centric warfare. The Army is still investing heavily (hundreds of millions) in trying to conduct analysis and fusion of raw data forward in expensive shelters and closed networks that connect through very low bandwidth pipes to everyone else. This effort ignores the role of cognition in converting information into intelligence and the power of networking in a high bandwidth environment.

The consolidation of sensors that require vastly different flight profiles onto a single overpowered platform while not increasing the number of platforms or filling the voids this effort creates reflects lack of understanding of the adversary's systems or collection requirements over time. The lack of interest in close access SIGINT has left a gap in the capability to perform persistent conventional and unconventional collection in those efforts that support combat and stability type operations. The most important finding of all is the lack of investment in training soldiers. The Army has moved away from training people to make informed decisions through leveraging technology toward training people to feed machines that support targeting.

Key Terminology

There is key terminology used throughout the monograph that is useful to define up front. *JP 1-02: Department of Defense Dictionary of Military and Associated Terms* defines information as "Facts, data, or instructions in any media or form".[40] *JP 1-02* defines intelligence

40 JP 1-02: Department of Defense Dictionary of Military and Associated Terms, 254.

as "1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning [the adversary] foreign countries or areas. 2. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding".[41] Intelligence is predominantly the result of a cognitive process and is a specialized kind of knowledge. Everyone with access to the adversary's systems and activities can collect information and input it into a network but an intelligence specialist is often required to convert special types of collection into forms before posting this to a network. Intelligence is the conversion of information into an accurate understanding of adversary activities and intentions. Anyone who does this is performing intelligence. However, those who know the enemy well perform the best intelligence.

FM 3-0, Operations defines the common operational picture is "an operational picture tailored to the user's requirement, based on common data and information shared by more than one command. The COP is displayed at a scale and level of detail that meets the information needs of the command at a particular echelon."[42] *JP 1-02, Department of Defense Dictionary of Military and Associated Terms* states that the DOD intelligence cycle "describes the process by which information [whatever its source] is converted into intelligence and made available to users."[43] Collection of information supports both the common operating picture and intelligence production. In a network-centric environment, information about the enemy is immediately available for the common operating picture. It is up to the decision maker if he/she wants to wait for the intelligence analysis to help refine the picture or whether this adversary is so immediate, or obvious that a commander chooses not to wait.

The *Joint Forces Command Glossary* defines operational net assessment (ONA) as a "continuously updated operational support tool that provides a JTF [joint task force] commander

---

41 Ibid., 261.

42 FM 3-0, Operations, 11-14.

43 JP 1-02, Department of Defense Dictionary of Military and Associated Terms, 262.

visibility of effect-to-task linkages based on a "system-of-systems" analysis of potential adversary's political, military, economic, social, infrastructure, and information (PMESII) war-making capabilities… its purpose is to identify key links and nodes within the adversary's systems and to propose methods that will influence, neutralize or destroy them and achieve a desired effect or outcome."[44]

Shulsky states that "Fundamentally, intelligence seeks access to information some other party is trying to deny. Obtaining that information directly means breaching the security barriers that the other party has placed around the information."[45] Access is a useful term since it is referring to the linkage of collection effort to specific types of information. That is information on the adversary's systems not just the collection of information.

Employment of a platform and sensor to collect in the adversary environment will most likely result in the collection of information – huge quantities of it. However, this does not equate to the ability to access or even the potential ability to access to information needed for full spectrum dominance. If the adversary (i.e. Al-Queda) does not use a particular communications system, you can spend billions of dollars and generate thousands of reports but none of this collection has access to the adversary's systems. Understanding the adversary's systems and is fundamental to the collection of actionable intelligence.

---

44 Joint Forces Command Glossary, http://www.jfcom.mil/about/glossary.htm, accessed 12 November 2003.

45 Abram N. Shulsky and Gary J. Schmitt, Silent Warfare: Understanding the World of Intelligence, (Washington, D.C.: Brassey's Inc., 2002), 172.

Sensors, Platforms and Access to the Adversary's Environment

This chapter is a general examination of the physical domain of the adversary and the ability of sensors and platforms to access the adversary's systems (political, military, economic, social, infrastructure and information) and its environment. The primary purpose of this chapter is to provide those not familiar with these systems a brief introduction to them. The focus is not on the details but understanding the relationships and principles of employment.

It examines the ability of technology to provide information at the level of fidelity (time and space) a land maneuver force requires. It examines physics, orbital mechanics, political geography, natural barriers and relationships between systems. We will not go into great depth but instead establish the general capabilities and limitations of technology. [46] The focus is on understanding the ability and relationships of these systems to support Army requirements. According to Gharajedaghi, "When we understand something, we no longer see it as chaotic or complex."[47]

Space Collection

Space based collection platforms and sensors support strategic and operational level collection requirements well. They are wide area collectors and provide global detection and cueing for other collection means. They can provide a great deal of information on infrastructure, terrain, and large-scale activities. Their primary purposes are to collect on denied areas of the world where there is no other practical solution in support of strategic decision makers. They were originally creations of necessity resulting from an information war between the U.S. and the

46 Specific technical capabilities, absolute values and limitations of individual sensors and platforms are among our most classified secrets. However, the laws of physics that govern the theoretical maximum capabilities of these systems and the barriers to collection are not. The secrets are how close these elements approach the theoretical limits, specific technical capabilities and how successful they are in penetrating the environment or barriers an adversary throws against them.

47 Gharajedaghi, 25.

Soviet Union.[48] The U.S. had no information on the capabilities of the Soviet bomber and nuclear missile programs (among many others). Space collection provided the only practical solution.

Improvements in satellite imagery collection are occurring yearly through improvements in technology and by the expansion of collection into non-visible wavelengths of light (multi-spectral imagery) which enables the extraction of information from the environment that was not possible with older space systems. However, satellites have very limited abilities against most tactical target sets. The ground force is mostly interested in mobile targets and relatively tiny pieces of the earth. Satellites only have visibility to the tiny piece of earth in which tactical forces are interested in for a short time. According to Peebles, "They cannot escape Kepler's laws of orbital physics. A satellite's orbit once established remains fixed, making movement as predictable as the rising and setting of the sun."[49] A satellite cannot park itself over the battlefield. It must circle the earth continually or gravity will drag it down.

The best resolution imagery comes from placing a satellite in a low earth orbit. There is no magic in this. The closer you take a picture the more detail it has.[50] Unfortunately, at this low altitude a satellite is traveling up to 18,000 mph. In a single orbit, an optical sensor on a satellite would have visibility on a tactical target (i.e. a tank) for only a few minutes at best during each rotation. For the other 95 percent of the orbit, it is not collecting information of value to an individual tactical commander although it is supporting someone else. Fortunately, there is more than one satellite but far less than the multitude required for the persistent surveillance a tactical commander needs.[51]

---

48 Curtis Peebles, High Frontier: The United States Air Force and the Military Space Program, (Washington, D.C.: U.S. Government Printing Office, 1997), 1.

49 Ibid., 156.

50 The shorter the wavelength (higher the frequency) the greater the resolution the imagery has. Visible light has a shorter wavelength than infrared light or radar so it will have greater resolution.

51 What the Air Force and Navy call persistent surveillance does have the same meaning for a Unit of Action commander. The amount of detail each needs to accomplish their mission is also vastly different. The time that the information collected is of value is vastly different depending on who you are. A picture taken of adversary terrain may be good for weeks and years at the strategic level. At the operational level, it may be good for

The earth is also rotating under the satellites' orbit. Therefore, the sensor will have a different aspect angle on the target the next time around. The target might not be in view at all on the next pass if there are obstacles obstructing that aspect view. The target could also simply move. If it took 90 minutes for a satellite to circle the earth, the target could move 90 minutes away in any direction. This is even worse if the adversary knows when it is in the view of a satellite; it can simply hide for those few minutes. Sophisticated adversaries and their allies know the orbits of our collection satellites. What we hope they do not know is how good (or bad) these are at accessing their systems.

If the distance (size of the orbit) is increased, the time over the target is longer (more pictures). However, the time to complete a rotation also gets longer. This increase in revisit time gives the adversary more time to move before this satellite returns. Distance also affects resolution of imagery. The desire to balance the competing demands between those who want more time over the target (wider area coverage but lower resolution) with those who want higher resolution (narrower field of view) resulted in elliptical orbits in the original imagery satellites.[52]

The most important thing for a tactical commander is time. Knowing when an overhead system will be in line of sight of the target area is important. Knowing if the platform can provide the level of resolution to answer the question is also important (weather, angle, distance, obstacles all play a role in this). However, if the time from collection to the delivery of actionable knowledge is too great, a picture of the same area taken a week ago or no picture at all is just as good. This highlights two very important points. First, to meet tactical time requirements requires an extremely robust exploitation organization in a high bandwidth environment, lots of processing power, and lots of imagery workstations all focusing on the commanders requirements the moment an overhead image is available. Second, if tactical commanders already have detailed

---

hours. At the tactical level, it may only be good for a few minutes. Some events, like a missile launch, are only good for minutes at all levels especially if they are the intended target.

52 Richelson, 201.

imagery and maps, they do not need annotated imagery that consumes vast quantities of both time and bandwidth. They just need the information and intelligence on the adversary.[53]

The ability to collect and locate the origin of tactical signals on the ground from space is difficult. The term tactical here refers to low power, short duration communications between adversary forces that are mobile or semi-fixed. Even if space assets could perform this task it would probably produce an area not a point location of these.[54] Flooding the tactical unit with this low fidelity information is also counterproductive. Fortunately, the strength of space reconnaissance is in global detection and cueing. They have the ability to assist in detecting where and how the adversary's systems are vulnerable to collection by other means.

A tactical signal is anything from a hand held radio bought at a local retail store to conventional military radios mounted in combat vehicles. The important point is that the power of these transmissions is low and the variety of their waveforms and internal content is as varied as technology allows. To intercept a signal, the system collecting it has to match the system sending it. Since satellites take years to design, build and launch, it is not economical to build them to collect on these types of systems. Technology is changing too fast. The Air Force is building unmanned aerial vehicles (UAV) that will have the flexibility to adjust rapidly to changes. It is easier to change a payload on a UAV than to launch a satellite. However, even these fly at too great a standoff distance to locate and apply persistent surveillance of tactical emitters.

To extract actionable information from space requires the correct architecture and a responsive and robust intelligence organization to exploit that small window of time that satellites provide information of tactical value. A human mind is integral to converting this information into actionable knowledge. While automation can assist by identifying possible targets, classifying signals and comparing images for changes, it has not yet replaced the human. We

---

53 Placing imagery exploitation assets into an austere environment to perform analysis severely limits their performance. In a high bandwidth environment, imagery analysts can access years of historical data of all types that would take weeks or months in an austere environment.

54 The upper atmosphere deflects, diffracts, reflects, and absorbs low frequency signals making it hard to pinpoint where it is coming from. Distances, power and propagation paths also make it hard.

highlighted that satellites are poor tactical collectors due to their orbits and great distances but they provide invaluable support in other areas. Among these are communication systems for command and control, wideband broadcasts, friendly force tracking, navigation systems, meteorological collection, digital terrain mapping, geological studies, and early warning of high-energy events.[55]

Aerial Collection

Although Benjamin Franklin predicted the use of balloons in warfare in 1783, it was not until the American Civil War that this nation used balloons to perform observation duties in combat.[56] However, balloons where vulnerable to small arms fire so they did not get close to the front lines, which nullified much of their altitude advantage. Their bulky gas-generating apparatus also prevented them from maneuvering. Armies displaced faster than the balloons could reposition. The use of balloons stopped in 1863 well before the war was over.[57]

The next significant use of aerial platforms for intelligence collection was in World War I. They were too small for delivering many bombs so their greatest role was initially in reconnaissance. Photography required chemicals to develop the film. Therefore, there was no real time imagery. Maneuverability, line of sight, and logistics were not big problems for the airplane. However, aerial reconnaissance gave birth to aerial combat. Their greatest difficulty was communications and coordinating activities. At the beginning of the war, they were dropping messages. By the end, both sides were using wireless telegraphy to adjust artillery fire.[58]

---

55 Peebles, 32-40. High-energy events are things like missile launches. The Defense Support Program (DSP) control satellites equipped with infrared sensors that maintain constant surveillance of the Northern Hemisphere. Their high altitude (2,000NM) produces low-resolution infrared imagery.

56 Alfred F. Hurley, William C. Heimdahl, "The Roots of U.S. Military Aviation in Winged Shield, Winged Sword: A History of the United States Air Force, vol. 1, 1907-1950, ed. Bernard C. Nalty (Washington, D.C.: Air Force History and Museums Program, 1997), 3.

57 Edwin C. Fishel, The Secret War for the Union: The Untold Story of Military Intelligence in the Civil War (Boston, MA: Houghton Mifflin Company, 1996), 443.

58 Daniel R. Mortensen, "The Air Service in the Great War" in Winged Shield, Winged Sword: A History of the United States Air Force, vol. 1, 1907-1950, ed. Bernard C. Nalty (Washington, D.C.: Air Force History and Museums Program, 1997), 36.

World War II was a leap ahead in the use of aerial reconnaissance. It saw the merging of large quantities of all sources of intelligence to develop detailed collection plans and the coordination of all the assets in a focused manner. Airborne signals intercept platforms were direction finding, identify radars and intercepting high power radio communications. Instead of imagery aircraft wandering over terrain looking for high value targets, SIGINT was steering their collection effort. SIGINT provided access to the adversary's most sensitive targets due to the breaking of their codes.

Wide area imagery reconnaissance was still required to locate key industrial targets, create maps, and determine tactical dispositions. Imagery interpretation was in three phases. The first phase supported situational awareness and initial Battle Damage Assessment (BDA). The second phase looked for less obvious targets in the imagery by more experienced personnel. They compared images of the same area from different days to look for clues of other activity. The third phase was the most detailed. It involved experts who had watched or studied the area or target in tremendous detail. These individuals performed detailed analysis of the adversary's systems to determine where to bomb and could assess the effects of bombing.[59]

For the next forty plus years, the Soviet menace drove our collection platform designs and the design of our entire intelligence community. Their vast country and tight borders posed a serious collection problem. Early attempts to send balloons over Soviet territory proved impractical. They flew in unpredictable paths and their tendency to land in adversary territory made them a political liability.[60] There were deep reconnaissance missions of Soviet airspace by high altitude bombers carrying collection equipment through the early 1950s. The Air Force

---

59 Alexander S. Cochran, Jr, et al., Piercing the Fog: Intelligence and Army Air Forces operations in World War II, ed. John F. Kreis (Washington, DC: Air Force History and Museums Program, 1996), 57-85, 422.

60 Curtis Peebles, High Frontier: The United States Air Force and the Military Space Program, (Washington, D.C.: U.S. Government Printing Office, 1997), 2.

admits that these missions occurred but the details are lost to history.[61] There were similar flights over China during the same period.[62]

The next effort was the employment of the Lockheed U-2 aircraft, which could fly as high as 70,000 feet armed initially with optical cameras. Its major success was the verification that the Soviet Union was not building a large bomber force.[63] However, after its shoot down inside the Soviet Union in 1960, it was limited to only peripheral flights. The U2 continued to operate over China but Chinese Nationalist pilots flew these missions.[64]

The Air Force and Central Intelligence Agency knew that the U2 was vulnerable. This vulnerability led to a secret effort to build a supersonic low radar cross section aircraft: the SR-71 Blackbird.[65] It was already in production to replace the U2 at the time of the shoot down. Its normal operating altitude of 80,000 feet and speed of over 2,200 mph made it extremely hard to detect (or at least early enough) to intercept it.[66] It could literally cross the country before they could adequately respond with missiles or aircraft. It could carry three state of the art sensors: optical cameras, high-resolution radar, and an electromagnetic reconnaissance system (radar signal collector and identifier) but it never performed its intended mission.[67]

Three factors prevented the SR-71 Blackbird from becoming a viable solution: it cost over $70,000 per flying hour as opposed to $1,200 for the U2; the success of satellite systems; and the continued downing of manned reconnaissance aircraft.[68] According to a National Security Agency publication, *National Aerial Reconnaissance in the Cold War,* there are "thirty

---

61 Vance O. Mitchell, "U.S. Air Force Peacetime Airborne Reconnaissance During the Cold War, 1946-1990." In Golden Legacy Boundless Future: Essays on the United States Air Force and the Rise of Aerospace Power. Edited by Rebecca H. Cameron and Barbara Wittig. (Washington D.C.: US Government Printing Office, 2000), 149.

62 Jeffrey T. Richelson, The Wizards of Langley: Inside the CIA's Directorate of Science and Technology, (Cambridge MA: Westview Press, 2001), 19.

63 Peebles, 5.

64 Richelson, 54.

65 Richelson, 20.

66 Mitchell, 148.

67 Paul Crickmore, Combat Legend: SR-71 Blackbird, (Shrewsbury, England: Airlife Publishing Ltd., 2002), 17-20.

68 Mitchell, 155-156. An Air Force RB-47 was shot down in the Barents Sea two months later.

documented Soviet attacks on U.S. reconnaissance aircraft [during the Cold War]. A tragic thirteen were successful".[69] The Cuban Missile Crises also lessened the political viability of penetrating the Soviet Union with a supersonic aircraft.

There is a wide variety of airborne collection systems. We will divide them into three categories based on their primary mission and the levels of decision makers they support. There are strategic, operational and tactical collection platforms. Some can also perform dual roles. These aircraft fly in particular flight profiles to place their sensors in a particular geometry based on a detected vulnerability either from space or airborne surveys of the electromagnetic spectrum.

Strategic platforms include the Lockheed U2, its replacement the RQ-4A Global Hawk UAV, RC-135 Rivet Joint, EP-3 Aeries II. They are employable worldwide on short notice. They are all very high altitude aircraft that enable them to peer as deep into adversary territory as possible. Peacetime reconnaissance operations (political boundaries mainly the Soviet border) drove their design and function. Their high altitudes and/or single platform employment profiles make them poor tactical level systems. However, they do have operational level utility during the early stages of combat. When air superiority is established and/or the ground force enters, they cannot compete with the lower altitude collectors for imagery resolution or signal location accuracy. Processing and exploitation occur on the aircraft or at fixed processing facilities prior to posting onto a network. Many of the things they collect on are too sensitive for other than intelligence organizations to see except when they are in an operational support role.

Operational collection platforms are those primarily designed to support conventional combat operations against land conventional forces. These are primarily the E8 JSTARS which provides moving target indications and synthetic aperture radar, RQ-1 Predator imagery platform, and the RC-12 Guardrail Common Sensor (GRCS) system which is a high accuracy SIGINT collection and location system. There are a few others but they are associated with special

---

69 National Aerial Reconnaissance in the Cold War, (Fort Meade, MD: Center for Cryptologic History, 2000), 4.

activities. The strategic platforms mentioned previously and satellites support these platforms with detection, cueing, and tracking. These platforms provide superior collection in support of conventional combat but are very limited in supporting stability operations.

Guardrail was originally a persistent tactical level collection and targeting system. However, its usefulness in that role has diminished gradually over the years. Since this is an Army system, we will cover it in detail in the analysis chapter. The E8 JSTARS has personnel onboard who are susceptible to fatigue. Its oblique collection angles make its sensors vulnerable to obstacle masking. Mountains, hills, trees, buildings all interfere with collection. It is good for wide area surveillance of open areas.

The Predator UAV generally uses a relay satellite to perform its mission. This limits the number that can operate in a given area due to intense competition for relay satellites and frequency de-confliction with other Predators is challenge. The Air Force armed a few of these to support special operations. In this configuration, a laser designator on the aircraft can laze targets for it two Hellfire missiles or for another platform to deliver missiles or bombs to the target. Its electro-optical camera can support ground forces but its relatively high altitude is no match for the high-resolution imagery provided by low altitude tactical UAVs.

Tactical unmanned aerial vehicles (TUAV) includes the Hunter, Shadow, and Pioneer UAVs.[70] These UAVs also use ground data links, which means that they do not have to worry about satellite time but they do have to worry about frequency de-confliction with each other when in close proximity. The F-14/F16, AH-64 Apache, OH-58D Kiowa are manned aircraft that also support tactical combat collection. All of these aircraft fly much closer to the earth and provide a higher level of imagery resolution to land forces than operational and strategic platforms.

---

70 There are a number of UAVs projected to fly in the Unit of Action but they are supporting local collection efforts. For our purpose, they are part of the discussion on the Unit of Action.

It is at this tactical level that communications bandwidth begins to play a significant role. The UAV broadcasts information directly from the aircraft to those within range and with the equipment to receive it. It also sends the same information down a data link to a ground station. Those in the ground station controlling the UAV flight have the additional responsibility of converting imagery information into a digital text form (due to limited bandwidth) and disseminating this through the tactical network. Those receiving the direct broadcast from the aircraft are generally those most interested in the collection and within range to act on it.

However, terrain and vehicle movement can block this broadcast at critical times. [71] The general broadcast does not ensure delivery to those who may need it most or they simply may be too busy to recognize the raw information for what it is. The text version ensures delivery into those systems that are maintaining the Common Operating Picture (COP) and into the intelligence system for analysis. According to Witsken, "The key factor in the usefulness of the TUAV is how well its information is analyzed, interpreted and disseminated. Essentially, the TUAV must be embedded into the unit's command and control process."[72]

Most tactical level imagery is too unwieldy to handle within the tactical internet. It is easier to send imagery back to the fiber portion of the GIG, through a dedicated point-to-point satellite links, and then rebroadcast this through a wideband satellite than it is to send it horizontally in the tactical battlespace.

Ground and Sea Based Collection

There are strategic and operation level ground collection systems but most of these perform special activities, which are not part of this study. Some monitor foreign broadcasts such as radio and television programs. Others perform collection on very specific adversary system

---

71 Some of the controls and video in the smaller systems like those projected for use in the Unit of Action is unencrypted. This means that an adversary with only basic technical knowledge can leverage the video for itself or even steal the aircraft by simply having a stronger signal. Even two friendly units in close proximity can have the same effect on each other.

72 Jeffrey R. Witsken, "Integrating Tactical UAVs Into Armor and Cavalry Operations." Armor Magazine (March-April 2003): 37.

vulnerabilities. These normally do not support Army maneuver forces directly. These are extremely useful in support of stability operations since they can gauge the effectiveness of information operations and access specific systems. However, due to their special nature they normally support Joint Task Force or higher collection activities.

Sea based collectors (i.e. ships and submarines) are limited by terrain just as land based collectors are. However, these are generally trying to collect on other naval or shore based systems. Primarily they support the Navy and other strategic decision makers.

The Army currently has a single ground signals collection system called the Prophet system. It is a stand-alone system with a limited dismount capability. It current has no ability to fuse its collection effort with aerial platforms and other distant ground systems for greater signal location accuracy. There is a relatively recent effort to connect this with a payload employed on a Blackhawk helicopter but this was one of the weaknesses of its predecessor. Helicopters are too vulnerable for jamming missions and for survival require terrain masking. This makes them poor SIGINT platforms. The Hunter UAV was once going to carry SIGINT payloads but its termination stopped this effort.

The Prophet system does have a wider frequency collection range and a greater signal identification capability than the system it replaced. However, making linear comparisons is probably a mistake. The system it replaced was able to work as a larger system-of-systems enabling it to net with other ground collectors and an airborne collection platform. This made it a powerful system for both direction finding and coordinated jamming. This system also has no organic linguists unlike its predecessor.

The Long Range Surveillance units in the Military Intelligence Brigades do provide a persistent ground observation capability against specific point targets. However, avoiding contact with the adversary is their specialty. Interacting with civilian populations in stability operations is not one of their strengths.

The Unit of Action collection systems within the Stryker Brigade and those projected for the Future combat system predominately support combat operations. The human intelligence (HUMINT) capability is oriented toward force protection not access to adversary systems and control. Most are very young and do not have either the training or life experience to make the kind of informed decisions to support the level of understanding to perform this task. Two obvious weaknesses stand out for the unit of action collection architecture. The first is the absence of large airborne platforms (and associated data links) to provide communication between its widely dispersed entities and rebroadcast of wideband satellite transmissions in close terrain. The second is the lack of integration of its sensors with those at the unit of employment level and strategic level. The discussion on SIGINT above is a case in point.

Emitters

The fundamental ingredient for network centric warfare to work is information. Information comes from collection. Collection requires placing sensors in a physical location that exploits the adversary's vulnerabilities. Vulnerabilities may be ones an adversary is not aware of or ones that are difficult to deny or defend. In combat operations, we create vulnerabilities and collection opportunities by taking down those systems and barriers they use to protect it. However, once these are down it takes other collection assets to exploit the new opportunities.

A platform simply places sensors in a position to collect. Where that platform collects from makes it highly specialized. Connectivity to a network is also desirable. A network provides the ability to transmit raw information to organizations where people using technology can fuse it with other information to produce actionable knowledge. This is primarily through three methods: satellite relay, ground data link, and air-to-air data links.

Figure one depicts general relationships between emitters and collection systems. The equation in the top right hand of the figure is a simplified link budget equation. It is a rough formula used to determine if there is a reasonable chance two radios communicating with each

other. The adversary controls one side of the formula and the design of the system fixes the limits of the friendly side. The take away from this is that for signals the distance between the target and the platform is the critical variable. If an airborne platform is too far away, it will collect a lot of information we do not want (noise) but it will not have access to the information we want.

The remainder of the chart simply highlights that the access angles and flight profiles of are vastly different which requires a greater variety of specialized collection platforms. Less variety is less costly but less efficient. Visual collectors generally require very high access angles. Communications collectors require placement of sensors in the propagation of the emitter signal but close enough to collect on it. Tactical commutations collectors have to be low slow and close. Tactical ELINT is a very low profile and very distant to place two platforms in a geometry to collect on the main beam and side beams.

Placing multiple sensors on the same platform makes sense for strategic platforms but the closer you get to the adversary a greater number and variety are required. Battlespace geometry is critical. Satellites flying around the earth can only see a target for a short time. Strategic platforms can collect for a little longer. Operational platforms can use multiple aircraft and their closer basing to collect for longer periods. Tactical collection requires persistent and high accuracy. Ground systems are persistent collectors but they require integration with others flying overhead.

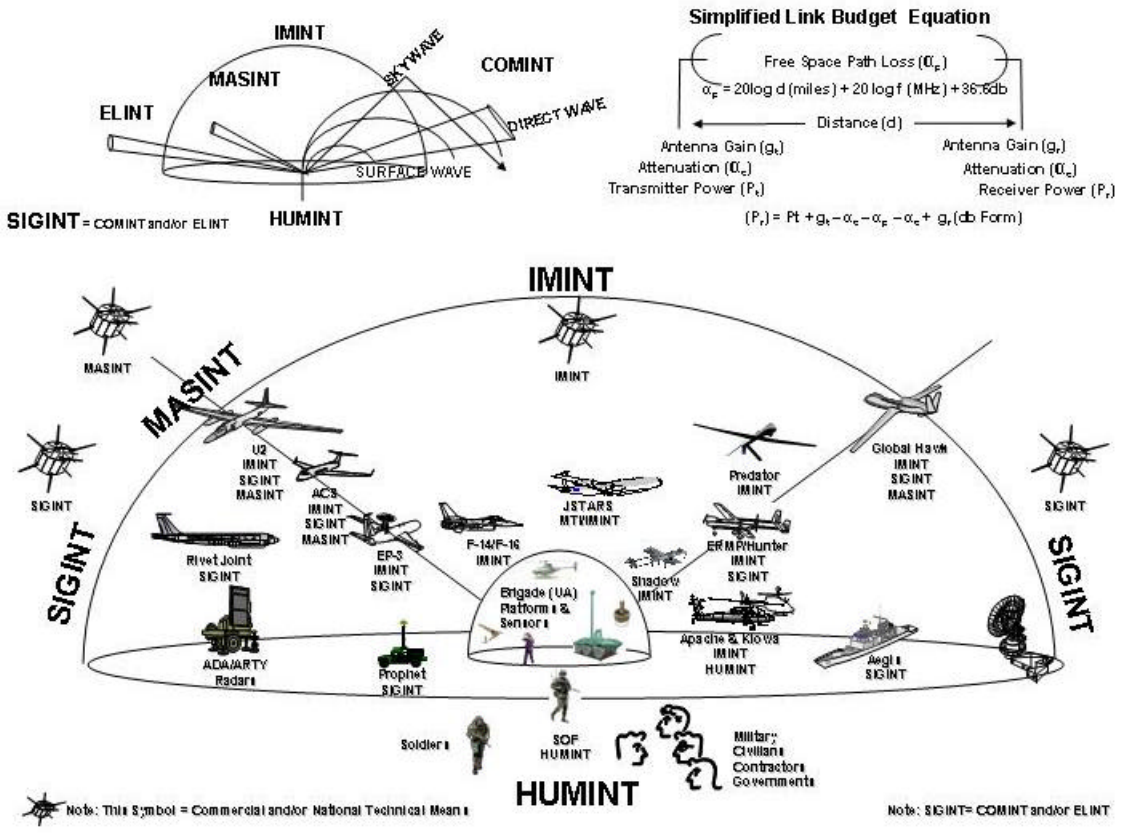


Figure 1. Battlespace Geometry

Summary

The purpose of this chapter was to examine the physical domain of the adversary and the ability of sensors and platforms to access the adversary's systems and its environment. The classification of many of the capabilities prevents detailed examination of some areas. Physics, orbital mechanics, signal propagation theory, political boundaries, battlespace geometry and enemy actions to deny access are the main limitations. We will finish this chapter with some generalizations about the relationships of collection systems that might help in understanding them better.

In figure two, the systems we have discussed in this chapter are on the top with the strategic systems on the left and tactical systems on the right. At the bottom of the chart are two additional elements of time and space. Strategic systems are generally focusing on collection that

supports decision makers who are looking at problems over years. These systems are extremely costly with huge overheads due to the great distances and relatively low fidelity access these have to adversary tactical systems. Tactical decision makers are dealing with problems that require decisions in the seconds and at very close ranges. Air Force and Navy are strategic and operational forces. The Army and Marines are primarily operational and tactical entities. There are other inverse relationships and directional relationships on the chart and many others not on it. The purpose of the figure is to depict the most common perspective of these systems. That is a linear or flat perspective without the dimension of time and as separate entities. The next chapter will focus on these as a system of systems with the added dimension of time to point toward gaps.

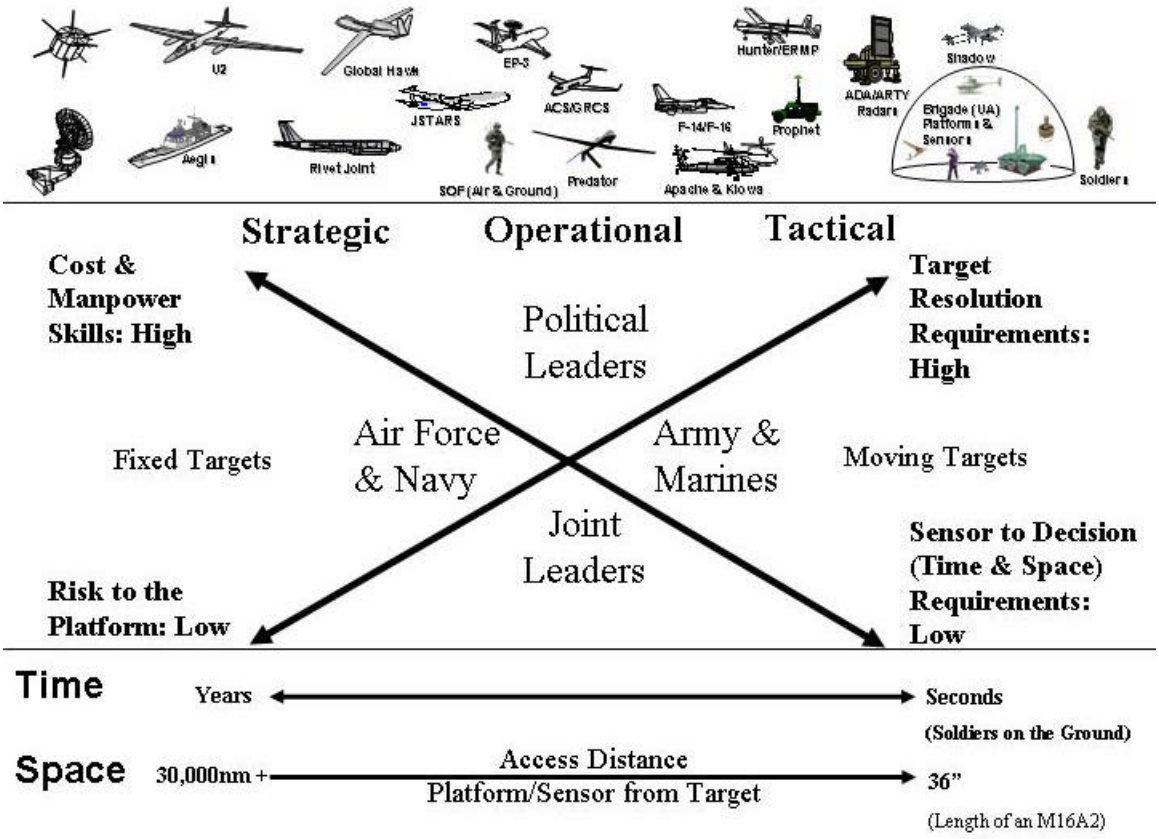


Figure 2. Relationships

Joint and Expeditionary Mindset

> We must immediately begin the process of re-examining and challenging our most basic institutional assumptions, organizational structures, paradigms, policies, procedures to better serve our Nation. The end result of this examination will be a more relevant and ready force – a campaign-quality Army with a Joint and Expeditionary Mindset.[73]
>
> General Peter J. Schoomaker, CSA, The Way Ahead

This chapter will describe a notional joint expeditionary campaign as a framework from which to examine the challenges of full spectrum dominance. The intent of this chapter is to show how collection systems described in the last chapter relate to each other over time. It will reveal why access to the adversary's systems and environment changes and why the value of the information products from these systems change as well. It demonstrates how systems' thinking[74] is essential to determining the requirements for Army airborne and ground collection platforms. It also provides a foundation for understanding the organizational, systems, and technical architectures needed to leverage the power of network centric warfare.

This chapter divides a campaign (or a war) into six phases: peace, prevention, deterrence, pre-combat, combat, and stability/support. These phases represent different collection access challenges and collectively represent the full range of operations a joint military force may face. There is no attempt to establish finite times for each phase. In the real world, these may run from days to years. In some cases, a land combat phase may not occur. A joint force may move directly into stability operations. On the other hand, in a large conflict, one area may already be in one phase while another is still raging in heavy combat. It is also possible for a stability operation to lead to combat and back again. There is some repetition of information from the previous chapter to reemphasis important points and relationships.

---

73 Schoomaker, 1.

74 Understanding the interdependence of these systems and seeing them as a single effort.

Peace

During peacetime, professionals in numerous government agencies at the strategic level are in a constant struggle for information against adversaries who are equally determined to deny or deceive their collection efforts. Shulsky argues that "intelligence is as much a struggle with an enemy as is armed combat; the difference lies in the means employed".[75] A competitive process based on political priorities determines the level of collection effort dedicated to a particular adversary due to a scarcity of strategic collection resources. It takes years to design, build and launch satellites. It takes just as long (or longer) to develop reliable human sources inside a terrorist organization or another government. If the adversary is a hard target like prewar Iraq, analyst may have to rely on low fidelity satellite systems, questionable human sources or whatever is in the public/private domains to analyze the adversary's primary systems.[76]

The intelligence community, other government and non-government activities are constantly building and maintaining databases on all aspects of potential adversaries for numerous reasons. However, due to resource scarcity (people and dollars), this effort may not be very robust before a crisis occurs. The major effort of military value during this time is the collection of facts on foreign tactical communication systems, weapon systems, military organizations, military exercises and conducting operational net assessments on primary systems. Technical reports derived from this effort form the basis for designing and building future collection systems and form the foundation for comparative analysis of activity over time.[77]

Due to geopolitical boundaries, satellites may provide the only information on denied areas of a country such as military facilities. However, Kepler's laws of orbital mechanics fix satellites in predictable orbits, which limit their ability to collect against tactical targets. Contrary

---

75 Abram N. Shulsky and Gary J. Schmitt, Silent Warfare: Understanding the World of Intelligence, (Washington, D.C.: Brasseys, Inc., 2002), 160.

76 Political, military, economic, social, infrastructure, information, …

77 Angelo Codevilla, Informing Statecraft: Intelligence for a New Century, (New York, NY: The Free Press, 1992), 4-15.

to popular myth, it is impossible to park a satellite above the battlefield.[78] Physics also severely limits the capabilities of space-based sensors to support collection against targets that have the ability to move and hide. For the land force commander, the greatest value provided by satellites in this phase is on neutral environmental factors such as geospatial information (three-dimensional maps), climatology data, fixed military positions, obstacles, infrastructure data, air defenses and general disposition of large military forces.[79]

Strategic level organizations through use of satellites and other means provide information on the adversary's systems that enable decisions on the types of sensors and platforms the Army should purchase.[80] General Hayden, the National Security Agency director, in testimony before congress described the problem of designing a SIGINT system: "A SIGINT agency [system] has to look like its target. We have to master whatever technology the target is using. If we don't, we literally don't hear him; or if we do, we cannot turn the beeps and squeaks into something intelligible".[81] This is actually an understatement of the problem from the tactical perspective. Even if the adversary simply reduces the power (or gain)[82] of its transmission, collection platforms may not be close enough (or its systems sensitive enough) to hear him. Visual line of sight is irrelevant if the power is too low or distance is too great.

Small-scale activities can occur unnoticed in full view of space systems if there are no indicators to focus exploitation. Background noise (signals and solar radiation) and clutter (optical resolution) hide many activities. Space assets are not good location systems for tactical emissions not only due to their low power but also due to the effects of the ionosphere on tactical

---

78 The only exception is a geostationary orbit at 22,300 miles directly above the equator. This is too far out for out for an imagery platform to provide resolution of any value to a tactical commander.

79 Jeffrey T. Richelson, The U.S. Intelligence Community, Fourth Edition, (Boulder, CO: Westview Press, 1999), 75-80.

80 William E. Odom, Fixing Intelligence for a More Secure America, (New Haven, CT: Yale University Press, 2003), 92.

81 Michael V. Hayden, Statement for the Record by Lieutenant General Michael V. Hayden, USAF, Director of the National Security Agency/ Chief, Central Security Service Before the Joint Inquiry of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence, 17 October 2002, accessed 21 December 2003; available from http://intellligence.senate.gov/0210hrg/ 021017/hayden.pdf; Internet.

82 'Gain' in simple terms refers to directionality of a signal which is also related to power. An antenna that broadcasts in all directions distributes power in all directions and therefore has a low gain.

frequencies.[83] However, they are great at detection, cueing, and tracking some activities until another system closer to the adversary emitter can pick up the mission.

Early warning is another significant activity of these systems. The value of this for the military commander never diminishes over time. Large-scale activities and abnormal events (i.e. missile launches, large military movements, etc. …) are relatively easy for the collective body of these sensors and platforms to monitor. However, there are limits in the numbers of overhead platforms, sensors, processors, analysts, and bandwidth. Therefore, a theoretical maximum capability also exists. Strategic level platforms (ground, air, sea and space) take years to build and have huge overheads. They do not increase in number or capability in times of crisis. This is why there are strategic air and ship platforms.

Strategic air and ship platforms also conduct routine collection missions but geopolitical boundaries generally prevent over-flights or encroachment of into territorial waters.[84] This means they also operate along very predictable paths (parallel to borders). Since position also indicates function, it is not hard to determine what they may be looking at. These flight profile restrictions make the access angles of their sensors susceptible to denial and deception and limit the depth of penetration or collection against the adversary. According to Mitchell "the overwhelming majority of Air Force reconnaissance missions during the Cold War skirted the Sino-Soviet bloc periphery. But their long-range oblique cameras could peer in only a limited distance, and under ideal conditions, the coverage against line-of-sight electronic transmissions was perhaps three hundred miles."[85]

---

83 The ionosphere absorbs bends, diffracts, scatters, and reflects many of the tactical frequencies which means they cannot always tell with any great accuracy where the signal is coming from. In practical terms, it makes no sense to try. Once the air and ground forces are no longer constrained by political boundaries, they can (if equipped) provide a degree of location accuracy and persistent collection unmatched by any space asset in these frequency ranges.

84 The Navy EP-3 midair incident and subsequent landing in China in 2000 is a well-known and highly publicized example of the overt nature of these surveillance activities.

85 Vance O. Mitchell, U.S. Air Force Peacetime Airborne Reconnaissance During the Cold War, 1946-1990. In Golden Legacy, Boundless Future: Essays on the United States Air Force and the Rise of Aerospace Power, ed., Rebecca H. Cameron and Barbara Wittig (Maxwell AFB, Ala.: Air University Press, 2000), 149.

However, since these platforms are closer to the target, below the earth's ionosphere and high clouds, they provide greater resolution to a variety of targets (less noise and clutter) and when combined with other sources help fill specific knowledge gaps. Many of the tests these systems were monitoring during the Cold War were too expensive to cancel just because one of our collectors showed up. The economics behind conducting denial and deception activities on the part of the adversary works in the favor of airborne platforms. It is sometimes just too expensive and too hard to cancel a test or a large military exercise.

Prevention

This stage begins when an event occurs in the diplomatic, informational, economic or even military domains that trigger a change in collection emphasis. However, at this point we do not want to let the adversary know we have a position or an interest in what is happening. In a volatile world, these events happen frequently. This movement into this phase could result from a news broadcast, intelligence cross-cueing or an economic event. On the other hand, it could result from an internal shift in political focus or desire to gather information to influence the target in some way. At this stage, the focus of collection is on gathering information in support of political decision makers for preventative (or pre-emptive) actions. There is no way to increase the number of strategic assets but it is possible to reallocate available resources to a single effort.

The benefit of National Technical Means (NTM) or strategic collection assets is that the adversary does not know if these systems are looking at them, looking somewhere else or not able to collect on them at all. However, employment of air, ship and other more overt collection efforts is a clear indication of our interest and therefore held in reserve at this stage. If they do not know we are collecting on them, there is a chance we might get lucky. Open source, passive strategic collection, or possibly covert collection methods are better choices at this stage. Submarines have always served as collection platforms to observe ship movements and coastal

areas. At the height of the Cold War, they served as signal intercept platforms and for wiretapping soviet underwater communications cables.[86]

At this stage, there is an increase in access due to collection emphasis and shift in resources such as workers. While analysts may classify a lot of the information collected as noise and clutter in this stage, it may prove of significant as the volume increases to a level where patterns begin to emerge. The value of the information a ground commander would place on this access is relatively high since there is no other information. The collective body of information up to this point would provide the foundation for military planning.

Deterrence

The effort of this stage is either to restore the political balance or to shift it to a desired outcome. The main effort is the application of pressure in diplomatic, economic and information domains. Information of all kinds supports this effort. Employing additional strategic and operational collection platforms or movement of military forces to a region is another way to send a very strong signal. The negative effect is that an increase in activity on our part will most likely increase denial and deception activities on the part of the adversary. The net effect will most likely force the unwanted activities underground or if we are lucky stop the activity. To mitigate these negative effects of show of force produces, significant collection effort during the prevention stage is essential.

Since the employment of operational collection platforms will affect behavior, activity and inactivity at various locations are telling. These changes may prove useful at uncovering other activities that where camouflaged by 'normal' routine. In other words, the 'normal' baseline created in the peace stage and augmented in the prevention stage creates a baseline to compare changes. The collection may also provide clues of where to search archives for information. A

86 Sherry Sontag, Christopher Drew and Annette L. Drew, Blind Man's Bluff: The Untold Story of American Submarine Espionage (New York, NY: Harper Paperbacks, 1998), 298.

sudden stop in normal activity in one area or an increase in activity in another is important for steering future collection and archive research. This type of collection is just like a police stakeout. You watch them for a while, stir them up and hope they make mistakes. These types of missions are not without risk. There have been numerous hostile engagements and shoot downs of our intelligence aircraft and hostile actions against our surface signals collection ships. North Korea kept the crew of the USS Pueblo for eleven months and never returned the ship.[87]

This is the stage when a ground force intelligence activities at the operational and tactical levels should start focusing on the adversary whether there is any intention of using a ground force or not. It is never too early to start learning as much about the adversary as possible and start creating the high fidelity databases a ground force requires. It is too late to wait for the pre-combat stage. The pre-combat stage in the future may only last a few days before soldiers are on the ground. Geopolitical boundaries still limit the depth of collection but the addition of more operational platforms increases the focus on military targets such as air defense assets. The quantity of useful information of value to the ground commander begins to increase significantly.

This is also the stage where it is critical for operational and tactical level organizations to analyze and compare current and archive data. Even comparing a picture taken twenty or thirty years ago to a current photo may reveal changes to the topography such as underground facilities. A collection event in the present may hold the key for the analyst to unlock secrets of the past.

Pre-combat

This stage begins with the clear intention or the real possibility of using military force. There is a substantial increase in the forward deployment of operational and possibly tactical collection assets along the periphery. However, there is also a marked decrease in the ability of strategic level assets to find, locate and determine exactly what the mobile elements of the

87 James Bamford, Body of Secrets: Anatomy of the Ultra Secret National Security Agency (New York, NY; Anchor Books, April 2002), 275-282.

adversary are doing. This is still a hard target to penetrate. Satellite, air and sea platforms are still operating on known paths and the ability to deny collection and hide activities through dispersal is very real. Joint-STARS aircraft have the ability to detect movement. However, terrain such as that in Bosnia or Korea with deep mountain valleys running parallel to flight tracks creates shadows that enable movement without detection. Many of our potential adversaries know the capabilities and limitations of our assets better than own ground commanders.

Although there is still little direct access to the adversary environment at this stage, the level of fidelity on targets of interest to the ground commander increases rapidly along peripheral areas to some depth. Large concentrations near the periphery are probably well known at this time but in the interior even large units can move undetected if they have knowledge of our systems (i.e. movement through dispersal) or are simply lucky. Dismounted and unconventional threats are extremely difficult to detect with standoff platforms unless they are in open desert terrain.

Combat

This stage is the application of all forms of military force. It is also at this stage that the invisible wall defined by political boundaries and defended by air defenses come down. Access to the adversary's environment and systems increases exponentially with the start of combat. However, the common picture of the adversary we had at the end of the last stage quickly dissolves under kinetic effects of precision weapons and effects based operations against adversary systems. The defeat or dispersion of large formations quickly follows but this does not make the collection any easier or the adversary picture clearer. It is at this point many hope airpower alone will defeat the adversary. In the future, we should probably expect the dispersion of the adversary's combat power from the beginning.

The very sources and targets of strategic and operational interest dissipate rapidly under kinetic and non-kinetic effects. Strategic and operational level assets simply run out of targets due to their own success and the relatively poor resolution of their systems. The ground force with

their close access to the adversary begins to provide more targets than their collection systems can find.

Shortly after the ground force commander enters the adversary's territory, he quickly realizes that higher-level commanders no longer have a better picture of the local battlespace. There is a precipitous decline in the ability of strategic and operational standoff platforms and sensors to access the environment to the level of fidelity needed by a ground force. The value of the information they provide drops rapidly. The ground commander's organic sensors become the primary source for meeting his or her information requirements. They also become the primary source of information for higher as well. The information they collect is feeding the targeting process. Dismounted adversary forces are able to move relatively free from detection and use built up areas and rugged terrain to negate standoff collection systems. More valuable and higher fidelity information is coming from soldiers not from standoff systems.

Prior to entering into combat, ground forces were the supported unit for information and intelligence on the enemy. The flow of information was down. However, when the ground force crosses into enemy territory, they are now a supporting unit for intelligence. This transition can overwhelm units if they do not train, equip and organized for it. The units that follow have to clear bypassed areas and need to know what the first units saw. Transportation units need to know the true condition of roads. Commanders and intelligence organizations all the way to national levels need information to steer support and collection efforts.

As time progresses higher will start to steer lower level collection assets to gather information they want. The ground force may find his/her UAV tasked to conduct battle damage assessment (BDA) missions for the Air Force. A Shadow UAV at a thousand feet has better imagery resolution than a Predator UAV at twenty thousand feet. Ground SIGINT platforms may have the only access. Even the best collection from the air cannot meet the level of fidelity that soldiers have on the ground. Soldiers can look under trees, in houses and in caves. The lower the

level of command the more marked is this effect. At the lowest level, it might appear that nothing of value comes from higher and they are constantly reporting up.

At the other end of the spectrum, strategic collectors become victims of their own success. The level of useful information from operational level assets also rapidly declines as targets disperse and adversary systems disappear. The dependence on information from tactical sources increases rapidly. The value of tactical sources is unmistakable. The information that took billions of dollars and years to collect is accessible for almost nothing once troops are on the ground. Stability operations, which are the topic of the next section, actually occur simultaneously with combat but last far longer.

Stability and Support

Destruction and defeat of the adversary's armed forces is the objective of combat. Control is the objective of stability (occupation) operations. However, Clausewitz wrote "Yet both these things [destruction of the armed forces and occupation] may be done and the war, that is the animosity and the reciprocal effects of hostile elements, cannot be considered to have ended so long as the enemy's will has not been broken." [88] The term occupation is no longer used but stability operations have the same goal of control and preventing an armed force from rising up. It is also not politically correct to talk in terms of 'breaking the enemy will' but of 'winning hearts and minds'. Winning hearts and minds or changing the enemy's mind is the goal of information operations. Combat, stability and information operations occur simultaneously. Collection for all also occurs at the same time. These require entirely different types of collection and very different types of skills.

Every combat commander should eventually find their units transformed into a collection unit and part of an information operation. In the stability phase, every soldier in contact

88 Clausewitz, 102.

with the population is a point of access both for collection and for dissemination of information. Their conduct and behavior, sends a message. A unit given a village, neighborhood or route to patrol has a collection and information operation role. This is not espionage but overt collection like a police patrol in a small town. Every soldier is a platform and sensor collecting information for themselves and everyone else. After a while, soldiers will get a feel for what is normal and hopefully will gain the support of the population. In the best scenario, the population will report activities to soldiers. However, this will not happen if soldiers hunker down in firebases or treat the population poorly.

National and operational level platforms and sensors can see major movements. It takes soldiers on the ground to assess the will of the population and to see into the dark corners. Caves, holes, jungles, cities and mountains require ground soldiers to penetrate. Soldiers are the ones collecting information on the close environment and feeding information into the network. This network feeds the common operating picture and feeds intelligence organizations to the highest strategic levels. This is not only limited to human collection but applies to signals as well. Access to local telephone lines or the ability to set up signal collection sites enables location and mapping of emitters. Even if a tactical unit does not have the skills or equipment to do this, it has created the potential for organization that can.

The information soldiers in tactical units collect from the local environment in turn steers higher-level collection efforts and steer information operations. These efforts in turn support these soldiers and provide feedback. The quality of support from higher at this point often depends on the quality of input from lower. If a tactical commander is not receiving intelligence, it may be that his soldiers are not able or willing to put information into the system. Local information is required to develop linkages to other sources of information, which results in actionable intelligence.

To access the environment at the tactical level requires cultural knowledge, observation, reporting, and interaction. These require training. Cultural knowledge provides a baseline for

knowing what is normal and not offending those you are protecting and observing. Just as a cop learns his beat, a soldier soon learns his or hers. Observation requires recognition of patterns of behavior and identifying cues from the environment. Reporting is also a skill that requires training. This is far more detailed than the Army SALUTE[89] report taught in basic training.

The type of reporting in this environment is more detailed. It establishes an information baseline for what is 'normal'. It includes details like names of individuals and their patterns. The day the janitor does not show up for work, the local mosque is empty, or children are not in the street is the day a car bomber might drive into your headquarters. In order to observe, soldiers have to interact with the population. In order to win hearts and minds also requires some form of interaction. Language skills are also important but not everyone need speak fluently. Everyone should know a few key phrases. There is also a requirement for very skilled intelligence personnel who know how to tie this overt collection to other human collection performed by trained intelligence personnel.

Conclusion

This chapter attempted to put the static descriptions of the last chapter into a joint context with the added dimension of time. The intent was to show how these work together over time to accomplish the same goal or full spectrum dominance. Strategic level intelligence collection and analysis begins long before the land force enters the fray and will continue long after it is gone. The ground forces needs to see itself as an extension of the existing strategic intelligence architecture not as a separate entity. If diplomacy is successful, then strategic collection was good enough. If airpower is successful, operational collection was good enough. However, if airpower is not successful, it will leave a dispersed adversary force and an increase in chaos and complexity. Only the close access a ground force provides can sort this out.

89 SALUTE: Size, Activity, Location, Unit, Time, Equipment.

Battlespace geometry is a critical dimension to collection potential. Once a ground force is inside the adversary's territory, it exponentially increases its access potential to the adversary's systems. This potential dwarfs all other sources, means and methods. Strategic and operational level platforms cannot match the level of fidelity or resolution a ground force can provide. Strategic and operational platforms reach a point in the combat phase where the ability to destroy targets is limited by no longer being able to observe or detect targets. As a member of the joint, interagency and multinational team, the Army then assumes a preeminent supporting role in intelligence collection whether it wants to or not. The collection assets of a ground force must support combat, stability and information operations simultaneously. The figure on the next page is a visual summary of this chapter.

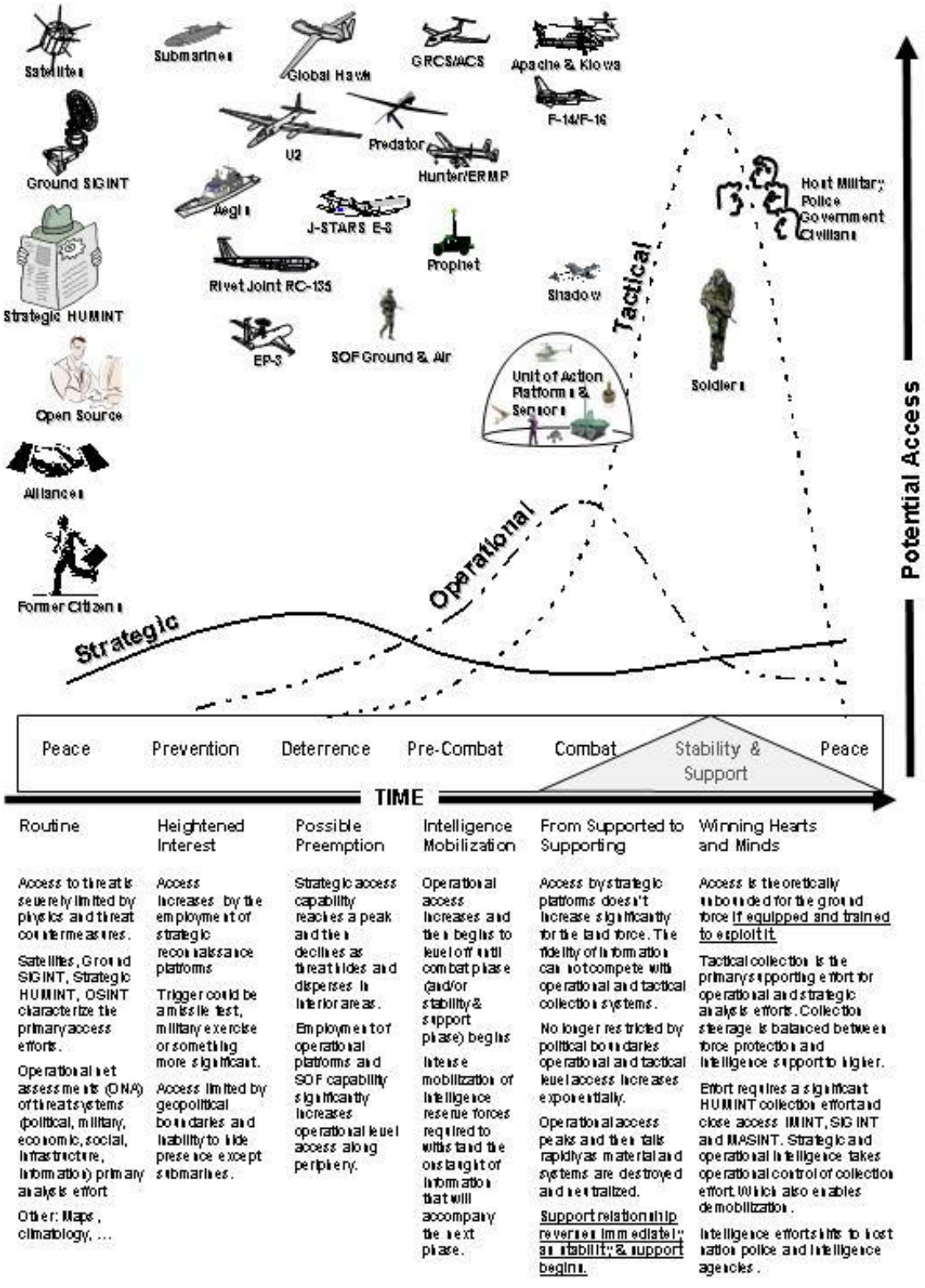


Figure 3. Potential Access Over Time

Analysis

> The data fusion myth blindly assumes the potential of complete automation at all levels, from data acquisition through insightful decision making (e.g., data – information – knowledge – understanding – wisdom – vision). Automation of these functions diminishes as the process proceeds from data to vision.[90]
>
> Bruce M. DeBlois

Full spectrum dominance is not the sole function of any one service or agency. It is an effort that involves joint interdependency at every step. The last two chapters attempted to narrow down the role of the Army in this effort. This chapter will attempt to narrow this further and then evaluate the ability of the Army to fulfill its obligation. Since this is a non-linear system, we developed what we called systems thinking criteria to assist in the analysis. In chapter one, we determined that full spectrum dominance requires collection systems that support the defeat of adversary's forces in combat. It also requires collection systems that support the control of the adversary in stability operations. In addition, it requires collection systems that support information operations.

Network centric warfare is a Department of Defense effort to increase the velocity of interactions between knowledge centers by creating a global information grid (GIG). The intent is to create a high bandwidth environment and standardized information exchange processes that will both increase the efficiency and effectiveness of our command and control (C2), and collection activities. The second part of the research question asked whether the Army's information collection efforts were in harmony with this concept. In chapter one, we determined that network centric warfare requires arranging the modular components of each collection system into configurations that maximize the power of the global information grid. These modular components equate to the different steps of the intelligence cycle. The power behind NCW is to increase the number of interfaces between nodes (knowledge centers) without

---

90 Bruce M. DeBlois, "Ascendant Realms: Characteristics of Airpower and Space Power," in The Paths of Heaven: The Evolution of Air Power Theory by The School of Advanced Airpower Studies, ed. Colonel Phillip S. Melinger. (Maxwell AFB, Ala:Air University Press, 1997), 557.

decreasing information velocity. Placing as many components of a collection system onto the high bandwidth portion of the GIG is the optimal solution.[91]

The last two chapters demonstrated that in the course of a military campaign, information does not flow in a single direction from all-seeing strategic and operational collection assets down to the tactical ground force. It is a dynamic collaborative process between all its members trying to manage scarce collection and communication assets. It is also not a fully automated process. In the description of the intelligence cycle, we discovered that data fusion and intelligence production requires a significant human effort. Both the common operating picture (COP) and intelligence analysis result from human decisions about what to collect, what to report and what to produce (display). Therefore, replacing people with technology is not a criterion of NCW. Increasing the interfaces between them (and computer processors) is. NCW does enable moving people to the fixed facilities (a high bandwidth environment) and decrease the forward footprint of some systems. However, it does not replace them. In fact, it enables the expansion of both human and automation efforts to help solve tactical problems.

Interdependence is fundamental to networking and a defining characteristic of a joint team.[92] With joint interdependence, there are also implied collection responsibilities based on the access advantages of each service and agency over the course of a campaign. While strategic collection is dominant before a campaign begins, the ground force dominates its final stages. The Army has a responsibility to report what it collects to the joint team as rapidly as possible. One of the problems with many of the Army legacy systems was their inability to share information.

The ground force has a singular collection advantage over every other service: the ground itself. The ground force has the potential to directly access almost every adversary system (most notably its social system) and challenge any collection barrier an adversary may throw against it.

---

91 Replacing people with technology is not a criterion of NCW. Increasing the interfaces between them (and processors) is. NCW does enable moving people to the rear but it does not replace them.

92 Schoomaker, 4.

Close proximity to the adversary provides it with the ability to apply persistent surveillance regardless of environmental conditions. It also has the ability to employ the best tactical collection platform ever contrived – the individual soldier.[93] Soldiers can move in any weather, they can run on empty for some time, and clouds rarely obstruct their visibility.

The advantages of a ground force when combined with the advantages of air, sea and space forces create powerful collection combinations. However, this is more than just running a communications wire between collectors and decision makers. According to Alberts, "It [network centric warfare] requires concepts of operation, C2 approaches, organizational forms, doctrine, force structure, support services and the like – all working together to leverage the available information".[94] It requires a systems view rather than a linear one. A systems view, according to Laszlo, "means thinking in terms of facts and events in the context of wholes, forming integrated sets with their own properties and relationships."[95]

For strategic systems, the value of collection and the ability to access the adversary's systems falls sharply in the early phases of a joint campaign and never recovers. For operational level platforms, the quality of collection and the access to adversary's systems increases rapidly with the establishment of air superiority and dominates the early stages of combat. However, this falls precipitously under the application of kinetic and non-kinetic effects. As large formations, fixed facilities and communications infrastructure disintegrate, disperse or hide, strategic and operational standoff systems become significantly less effective.

A ground force is not just a killing machine. It is also a huge information collector. As it spreads over the adversary's terrain destroying military equipment and personnel, it is also

---

93 A soldier can access environments (caves, jungles, mountains, cities) and access adversary systems that are difficult, cost prohibitive or impossible to do with standoff technology. A soldier equipped with language and cultural skills can penetrate the local social system and/or facilitate control of a local situation. A soldier equipped with technology (digital camera, signal intercept equipment, chemical detectors …) can provide all-weather persistent surveillance impossible with standoff technology.

94 David S. Alberts, Network Centric Warfare: Developing and Leveraging Information Superiority, 2nd Edition (Revised), 3.

95 Ervin Laszlo, The Systems View of the World: A Holistic Vision for Our Time, (Cresskill, NJ: Hampton Press, Inc., 1996), 16.

probing dark corners and connecting its sensors to critical adversary systems.[96] In effect, it is weaving a network of collection assets to contain and control the adversary and his environment. To defeat the adversary and control every situation, the ground force must constantly collect and update what it knows. This is not only to protect itself but it enables the preemption of any organized adversary effort. It is also not just the function of an intelligence organization. It is an Army wide responsibility.

Some believe that the mission of the Army is conventional land combat at the exclusion of those things incidental to it. Such a narrow view is to ignore the Army's history and its role as an instrument of national power. Army history is one of almost uninterrupted non-conventional operations interrupted by short periods of heroic combat. From colonial times through the nation's expansion to the west coast, the Army was a stability force performing primarily non-combat duties. With the nations' expansion of its sphere of influence into the Pacific, the Caribbean and with in its war with Mexico, both the Army and Navy performed occupation duties. The Army supported reconstruction after the Civil War, World War II and the Korean War. The failure of the Army to understand its role as a simultaneous controlling and stabilizing force probably contributed to its humiliation in Vietnam.

Another fundamental reality is that this nation is not going to create a separate occupation force to perform stability duties. While 'occupation' may be exactly what the Army does in stability operations, the idea of setting up occupation force is contrary to the founding ideals of this nation. Whether we want it or not it is a mission of the Army and always has been. This paper rests on the assertion that stability operations (and the unconventional warfare that occurs with it) are incidental to land combat operations and they occur simultaneously and sequentially. Further, the Army has the predominant responsibility for collection in this effort based on its proximity to

---

96 This could be as simple as establishing checkpoints on highways entering names and license numbers into a computer or the emplacement of an acoustic sensor along a road. These both monitor an adversary's infrastructure system. A signal collector tapped into a local communication fiber or linguists engaged with the local population are other examples.

the adversary and potentially unbounded access to the adversary's systems. The Army is a fighting, controlling, and stabilizing force. All of these efforts require collection of information on the Adversary across all phases of a joint and expeditionary campaign.

Collection Systems

The Distributed Common Ground System –Army (DCGS-A) is the Army's answer to network centric warfare for its collection systems. It will consist of three configurations: embedded in the Unit of Action (software), fixed facilities (knowledge centers) that reside on the fiber portion of the GIG, and a mobile portion.[97] We will focus our assessment on the mobile portion. The conversion of the Army's stand-alone programs into an interdependent system on the GIG is currently underway. It is roughly an $85 million dollar conversion program called the Interim Distributed Common Ground System – Army (IDGCS-A).

IDCGS-A is composed of Guardrail Common Sensor (GRCS), its replacement Aerial Common Sensor (ACS), the Army Tactical Exploitation of National Capabilities Program (TENCAP), Joint Surveillance and Target Attack Radar System (JSTARS) ground station, the Hunter Unmanned Aerial Vehicle and the Prophet system. We will look at each of the individual systems and then look at the at the IDCGS-A program and collectively evaluate these to support the goal of full spectrum dominance and network centric warfare.

Guardrail Common Sensor System (GRCS)

Guardrail Common Sensor System is the Army's manned airborne signals intelligence (SIGINT) collection platform. Its origins date back to Vietnam. The death of SP4 James T. Davis on 22 December 1961 highlighted the danger of moving into close terrain with short-range direction finding equipment. He was the first American soldier to lose his life during the Vietnam

97 U.S. Department of the Army. System Training Plan for the Distributed Common Ground Station – Army. (Ft Huachaca, AZ: United States Army Intelligence Center, Oct 2003), 1.

War. While the Air Force had airborne signals collection systems dating back to World War II, they were not able to DF against the low power tactical emitters to any degree of accuracy when they did intercept them. They were focusing on high power communications and radar emitters. Within three months, the Army had an airborne DF platform. By 1967, a single aerial exploitation battalion in had over 80 signal and imagery collection platforms (the largest today has only 15).[98]

These aircraft initially first flew as individual platforms with operators on board. They would manually triangulate the location of signals by talking with another aircraft. The next major development was the Army working with the National Security Agency to develop the configuration we see today. Two or three aircraft collect at the same time. Each has a data link that ties it to a common network. Operators are on the ground in air-conditioned vans able to rotate at will. Aircraft rotate off track to maintain persistent surveillance. This networking enabled a level of precision location of signals that is still unmatched. With two or three aircraft on track flying low, they could locate low power tactical and mobile emitters. It could also cue imagery collection platforms or ground personnel to the spot of the emitter.

However, a reduction in money and an end to the war led to a reduction in aircraft. This eventually led to the plan to put radar and communication collection capabilities on a single airframe and then reduce the total number of aircraft in the battalion. The Hunter UAV would take over the Imagery collection role once performed by the Mohawk aircraft. This all sounded like a great idea. However, several things happened. The Hunter UAV ran into trouble and they did not purchase more. The imagery aircraft were retired anyway.[99] For the Guardrail system, adding radar collection capability also meant adding more weight. This resulted in a bigger aircraft. However, a bigger aircraft burned more fuel and that meant that it must fly higher to get close to the same mission time for fuel efficiency. Flying higher required a pressurized aircraft

98 Army Security Agency Aerial Reconnaissance: Mission and Sacrifice, (Fort Meade, MD: NSA Center for Cryptologic History, 2000), 2.

99 Army airborne radar went with it.

and other things drove up costs. Money ran out to equip all the aircraft with mission equipment. The first version was incapable of carrying the extra weight of the radar collection system.

Collection of tactical communication signals and collection of tactical radar signals require significantly different flight profiles. There were three choices for the new platforms: fly in support of tactical communication collection; fly in support of tactical radar collection; or fly higher and change the collection mission. In isolation, a single aircraft looked more capable. It was a new pressurized aircraft but its standoff distance and altitude were growing. Its mission time was decreasing. They were no longer able to perform persistent collection missions for any duration. There were not enough aircraft in the system. From a systems view, there was a significant loss of total capability from a multi-system perspective and only small gains.

The compatibility between the systems was also a problem. Not all aircraft could fly with another system. Additionally, the newer aircraft could only deploy over the Atlantic in good weather.[100] To get to the Pacific they would have to fly around the world in the same direction. This would require diplomatic clearances of countries that might not want them traveling through their airspace or working in their region.

The helicopter signals collection system (Quickfix) was also getting too expensive to maintain. The ground systems it netted with to perform tactical signal location and jamming were gone and its mission was questionable. It was finally retired. All the current Guardrail systems have the capability of leaving their mission shelters tied to a fixed facility and deploying only the aircraft and relay systems forward. The latest version had the capability of sending data directly from the aircraft to a satellite. The primary mission of these aircraft is in support of pre-combat and combat operations.

---

100 This requires hops between Newfoundland Canada, then to Greenland, then to Ice Land and finally to Scotland. This is was not an insurmountable problem only an unexpected challenge.

Aerial Common Sensor (ACS)

Aerial common sensor is the aircraft replacement for the Guardrail Common Sensor System. However, it is a mistake to think of it as a replacement. It is a completely different system with very different mission capabilities and flight profiles. Before we get into the analysis of this system, we have to point out an important fact. The selection of the G450 Gulf Stream Airframe has a direct linkage to its other primary role in the Army. It is also a Very Important Person (VIP) transport airframe. The Army made the decision that it would have one airframe for both missions. It has a great strategic and operational level collection profile with a 4,350 mile range which makes it world wide deployable. It has also has an average cruising altitude of around 40,000ft with cruise speed of 850kph. It has two jet engines that give it great fuel efficiency for long distance flights but terrible fuel efficiency for reconnaissance type missions. This is a great replacement for the Navy's EP-3 Aeries II and it might be a good replacement for the Air Forces aging RC-135 Rivet Joint. This definitely provides the Army a strategic reconnaissance mission capability.

This airframe will have no fewer than six different types of sensors each requiring vastly different flight profiles to optimize their collection potential. Most of which are not survivable in support of most conventional type combat scenarios. Some sensors will require very low overhead flights (or at least high oblique angles). This will decrease the fuel efficiency. The flight profiles for the sensors it carries are also very similar those that already exist or will exist in other service systems. If these are all feeding the global information grid, this does not make a whole lot of sense. This is even more puzzling if the Navy buys this system as well.

This system will not close the tactical SIGINT gap (persistent collection and location of low power and fleeting tactical emitters). It is simply incapable of flying slow and low to dwell in the collection range of these types of emitters. How it will work with other aircraft and provide the coverage the Unit of Action needs or link with the unit of action ground sensors is an

interesting question. The aircraft flight profile however would make it an excellent communications relay system for the unit of action.

There is a big difference from being able to collect many signals and access to signals of value. The farther a signal collection system is from an area the more it will collect whether it wants to or not. Its standoff distance also makes it easier for the threat to hide important signals under this noise. It is also another thing to DF to a high degree of accuracy. There are a lot more questions about this system than answers. However, this is the type of aircraft required to a fight a global war on terror. It can also support a wide variety of unconventional collection operations. It will have the same ground station capability as Guardrail. It will also have the ability to carry on-board operators, which will give it greater flexibility for some missions. There are two clear conclusions: This is a strategic collection platform not a tactical one. It still does not meet the unit of action requirements for a dedicated airborne tactical SIGINT system.

Hunter Unmanned Aerial Vehicle (UAV)

The Hunter UAV is a system that has an incredible history. It was initially a joint program between the Navy and the Army. However, it simply did not have the capabilities that the Navy would need and was too large for the Marines. By losing its joint status, it also lost support and protection from the Army. At the time, the Army needed money for modernizing its wheeled fleet. Military intelligence at echelon above corps (EAC) wanted to go with the Predator UAV and the tactical Military intelligence personnel were looking for resources to pay for the TENCAP systems, JSTARS ground stations and the All Source Analysis System (ASAS).

This system was originally an Israeli product with an Italian motorcycle engine. All the software was in Hebrew and therefore there was not a great deal of testing of the software after translation into English due to the pressure to field the system early. There were actually two different Hunter systems. The original system at Fort Huachuca was training students and the actual production model was still undergoing testing. The whole system was under tremendous

pressure to produce. This led to the whole program coming apart. There was a cross border flight into Mexico and then training crashes.

About this time, the Department of the Army and FORSCOM got involved. They ordered the release of one of the production sets to go to Fort Hood. The unit at Fort Hood would train them and determine whether the Army should keep it. However, a series of crashes at Fort Huachuca sealed its fate. The Army decided to terminate it. There was evidence of sabotage found (gravel in a sealed flight control compartment) and some design modifications made on control surfaces. However, no one knows for sure why the crashes stopped. At this point, there was no way to revive the program and there were a lot of bad feeling and stories about this system that were impossible to kill.

This was a good thing in a sense. The pressure was off. The soldiers worked out minor problems by changing maintenance procedures. Rotations to the National Training Center and flying in the airspace around Fort Hood created a wealth of knowledge. The system never had a serious problem since. It did have some losses due to human error but over all even these losses were well below those programmed. The reason its termination was a good thing is that the lessons learned from this program directly translated into the Shadow program a few years later.

Currently there is an effort to turn the Hunter into an armed UAV. One issue not addressed with this proposal is the lost collection time. When you add roughly 100 pounds (two Hellfire missiles) this platform it results not in a loss of time getting to and from the collection area but the time over it. If you have only six aircraft in a baseline, then your total system collection time degraded by over half. One alternative not considered is simply to have the UAV laze targets and another platform shoot the missiles. The UAV does not lose collection time by adding weight but increases efficiency by having another platform carry the missiles. Not a bad alternative to the 20 million we are going to spend just to modify a Hunter UAV and all the millions to sustain the training and capability.

From the discussion of the above systems, it should be apparent that the Army has a tactical SIGINT problem. It began to grow over a dozen years ago as the Guardrail platform grew in size and moved farther away from the battlefield. The solution is integral to the Hunter (or its replacement) and the ground SIGINT system we will discuss next.

Prophet

The Prophet system is a ground based SIGINT system. It is essentially a vehicular mounted intercept system with limited dismount capability. It is capable of intercepting and identifying a wider frequency range than the systems it replaced. It also has a limited ability to direction-find. As with all ground-based systems, it has problems with terrain.[101] What is missing is an air component. The systems that this one replaced were able to net with a helicopter to perform direction finding and jamming. To go after tactical targets requires the ability to net with other interceptors especially one overhead that is also capable of detecting the same transmitter. In an urban environment, a dismount capability that can net from a rooftop is probably essential. Direction finding is all about networking and placing multiple sensors within propagation wave at the same time.

Manned aircraft are too vulnerable in today's environment to survive close access collection of this type. Distance is everything when collecting against low power tactical emitters. A UAV that can carry heavy SIGINT payloads is essential to the ability to collect and net Prophet systems together. SIGINT enables steering of imagery and other assets to the target. The ability of netting multiple UAVs to perform this mission is also important. The Unit of Action sensors will have the same problem as the prophet system. Its UAVs are too small to carry SIGINT payloads. The Hunter (or its replacement) must fill this requirement. Linking with the ACS

---

101 The parallel between 1961 and now is interesting. At that time, the Army only had a stand-alone ground SIGINT system and the standoff profiles of the manned aircraft at the time were not able to collect on these tactical signals with any accuracy or persistence. The Prophet System and Aerial Common Sensor system reflect the same problem. After forty years, we are essentially back where we started. Although the ground and air systems are far more capable in other respects.

system is not a high payoff option except to inject collection into the GIG or to net a prophet system with Unit of Action sensors.

Along with this capability is the ability for the UAV to carry electronic survey equipment. The adversary is not using militarized equipment it is buying it off the shelf. The ability to send a UAV forward to find out what they are using is essential to force protection. If your SIGINT system is not able to match the adversary then it will not hear it. It is not enough to collect in the same frequency. It must match the polarization of the waveform among other things. This capability is essential to equip both the prophet system and the Future Combat System SIGINT systems with the right antennas and other modifications prior to entering an area.

Army Tactical Exploitation of National Capabilities Program (TENCAP)

Under the concepts of maximizing the velocity of information from collection to consumer, the Army TENCAP system (or at least the imagery portion) is not compatible with the concepts of network-centric warfare. The current architecture sends raw data forward to a van on the battlefield where processing, exploitation, analysis and production occur. It then has to disseminate these to consumers, which in this case is limited to consumers with proprietary hardware and software. The dissemination means even to this forward processing site is slow. The Future Imagery Architecture (FIA) has slower processing time at its ground station than the current systems and even higher bandwidth demands to send out the raw data.

We know from an earlier discussion of orbital mechanics that as soon as a picture or a signal is collected the clock starts. Under the current architecture, it comes from overhead to a fixed facility then out to a van for exploitation and analysis. If this took only ten minutes to complete this, it is already nearing its expiration point. The problem is that from the van there is no reliable way to get it to everyone who may need it. It best method would be to send it back through the small pipe and post it on the GIG, which it could then send forward by any number of routes. The problem is that to send imagery back would tie up the pipe bringing imagery forward.

Nothing in the system should handle the same information twice in any form. A more practical problem is that there are not a lot of imagery exploitation positions in a forward van.

Under the Network Centric Architecture, every Army power projection platform (i.e. Fort Bragg) will have a fixed facility with high bandwidth access to everything. On this fiber backbone, the unit of Employment will have a fixed facility that will no longer send information forward but will process it into products that can go directly to consumers in whatever form they want without having to use any propriety middleware. A fixed facility has the ability to add more than a couple of positions.

Since it is on a fiber backbone, a reserve unit at another installation could do this just as well. They would not have to deploy to do this either. From this facility, a product could go directly to a soldier on point though a broadcast. What should go forward are products not raw data. In a ground action more valuable information is flowing up not down. A simple analysis shows that doing the strategic processes on a high-speed network will get the products to those who need it faster. There is also the ability to leverage more workers for the cognitive processes involved with interpreting and analyzing imagery. What we have discussed is just first phase imagery analysis. Doing the more valuable research of the area is just not practical forward. Doing this stuff forward is neat but it is not smart. If you have the pipes to get raw data there, those same pipes will send products just as well.

Interim Distributed Common Ground System – Army (IDCGS-A)

Under this program, all the ground elements of the systems describe above with the exception the prophet system are supposed to merge into one huge modular system. The JSTARS ground station is also part of this merger. If we examine this from the perspective of the GIG this is may have been a step back. Instead of multiple stovepipes, we now have a big one. From a network centric perspective where the golden rule is information velocity, this creates more friction. While there is a lot of information flowing into this setup the horizontal distribution is

still limited. There Unit of Action will not likely be anywhere near this setup and the only reliable way to send this information forward is to send it back and then up to a satellite for broadcast. An airborne platform to relay this is not in the works.

The sources that feed the Army TENCAP systems originate from systems on the GIG.[102] Guardrail and ACS have the ability to work from fixed facilities on the GIG. One of the benefits of the GIG will be to enable the aircraft to fly forward in support of any Combatant Commander even another agency and they could control the sensors. It actually works better on the high-speed fiber. If you force this to go forward, you decrease not increase the flexibility and number of interfaces these systems have with other knowledge centers. Placement of analysis functions on the fiber backbone of the GIG allows the distribution of collection to more customers.

The Air Force is currently working on posting their JSTARS information to the GIG and increasing the number of air-to-air data links between its platforms. The Prophet system could inject into the GIG in a number of ways. Satellite communications, data link to an airborne platform such a Guardrail or ACS. The only thing left is the Hunter system (or its replacement). If it is a SIGINT system, it could net with Guardrail or ACS. Imagery is a problem but the reports produced in the ground system are not. Production of imagery reports is a basic function of those in the shelters and posting these to the GIG could occur though sending it to a guardrail or ACS.

Network centric warfare requires arranging those physical, cognitive and informational elements[103] of intelligence production into configurations that maximize the power of the global information grid. Instead of being a step forward the Interim Distributed Common Ground Station-Army (IDCGS-A) effort is a clear indicator that the Army does not understand what network centric warfare is all about. This program does not improve collection. It does not increase the number of nodes (it reduces it to one). It does not increase the speed of delivery of

---

102 Very little comes directly from a satellite and that which does also go onto the GIG as well.

103 Planning, direction, processing, exploitation, analysis, production, dissemination, integration, evaluation and feedback.

products (relative to a GIG solution described above). It also does not increase the number of dissemination methods.

On the GIG, there is the ability to increase the number of personnel to keep up with the flow and volume of information. It also enables the mobilization of information not people. If raw data goes forward, there is no choice but to let information go unexploited when there is too much for the limited personnel, connectivity or bandwidth to handle. This program appears to be an attempt to fix configuration management problems with legacy hardware and make propriety hardware and software programs work together on a local network. This has nothing to do with network centric warfare. It is actually the opposite. Instead of opening up the architecture, it is collapsing it.

For the land force, the potential ability to access any adversary system increases exponentially the deeper it penetrates into the adversary's territory. However, potential does not necessarily translate into ability. The Army's investment in collection during any phase is currently far less than its potential to access the adversary's systems. The majority of the Army's collection dollars are going toward leveraging systems that do not have a great deal of payoff where the Army needs it most: in the close fight and in stability operations. Overemphasis on standoff collection technology in support conventional combat operations has left it vulnerable in non-conventional operations. The Army mission is not only to defeat the enemy conventional forces in combat but also to control the situation in any type of military operation.

Conclusions and Recommendations

The purpose of this study was to determine if the Army's information collection efforts are supporting the goal of full spectrum dominance and if they are in harmony with the concepts of network centric warfare. Full spectrum dominance requires collection systems that support the defeat of the adversary's forces, the control of his environment and systems, with the strategic objective of defeating the adversary's hostile will.[104] According to Sun Tzu, "The best policy is to take a state intact. … To subdue the enemy without fighting… capture his cities without assaulting them and overthrow his state without protracted operations".[105] He goes on to state that, "the reason the enlightened … conquer the enemy …is foreknowledge".[106]

Information (foreknowledge) gained through access to adversary systems supports defeating the adversary's forces. This in turn provides potentially unlimited access to the adversary's environment and other systems. However, there is dissonance between the strategic goal of defeating the adversary's hostile will and tactical objective of defeating his forces.[107] The Army having sacrificed soldiers to achieve potentially unlimited access to the adversary's environment and systems currently does not have the collection capability to exploit this and control the adversary's environment and systems. Prior to the friendly land force occupying the territory, the adversary controlled all the information between the government, the people and the military. The friendly force must control the information between these three elements and all the

---

104 Clausewitz, 102.

105 Sun Tzu, The Art Of War, trans. Samuel B. Griffith (New York, NY: Oxford University Press, 1963), 77-79.

106 Ibid., 144.

107 There is evidence that the dissonance or 'cognitive tension' that exists between the strategic and tactical levels of warfare resulted in the operational level as argued in Shimon Naveh, In Pursuit of Military Excellence: The Evolution of Operational Theory (Portland, OR: Frank Cass Publishers, 1997), 4-14. One of his arguments (7) was that operational art was born from the need to use a systems approach to warfare to manage the complexity of linking tactical missions to strategic aims. His evidence focused on the operational art of defeating adversary formations. This study focused on collection systems that support both the defeat and control of adversary systems. The operational art of defeating our adversary is what drives training, organization design, and material development in the Army. However, the art of controlling the adversary environment and systems not even a mission recognized by the Army even though it is incident to land combat and a strategic objective.

systems that relate to them. It must then replace this information with its own. Information warfare is a contest for the control of information to the populations on both sides of a conflict.

Network centric warfare requires arranging the modular components of each collection system into configurations that maximize the power of the global information grid (GIG). The power of the GIG is not the fusion of data by machines. It is networking people and organizations in a robust interoperable high bandwidth environment to increase the effectiveness of those who make decisions about information. Cognitive actions of people not only machines are involved at every step of converting information into knowledge. Network centric warfare does not replace people it changes the location of where they are and how they interact with each other. However, this concept also assumes that there is access to, and collection on, the adversary's environment and systems. It also assumes that the people who are making decisions about information have the training and cognitive skills to transform the information into greater understanding and not greater friction.

In both full spectrum dominance and network centric warfare, the Army (from a collection standpoint) is not supporting either very well. While there are indications that the operational Army is beginning to understand and support these efforts, it is in the institutional Army where these have yet to take hold. The institutional Army is where lasting meaningful changes take place. Institutional culture and processes drive resource decisions that translate concepts into capabilities.[108]

After examining the Army's major collection systems, the expenditure of resources shows a tremendous amount of money on programs that are in direct contradiction to the concepts of network centric warfare. In the area of full spectrum dominance, there is a heavy investment in collection systems that support combat operations while there is very little investment in the

---

108 David A. Fastabend and Robert H. Simpson, Adapt or Die: The Imperative for a Culture of Innovation in the United States Army (Fort Monroe, VA: U.S. Army Training and Doctrine Command, 2003), 4-6.

equipment or highly specialized training required for collection in support of stability type operations.[109]

In stability operations, soldiers are in very close proximity to adversary's systems (political, military, economic, social, infrastructure, and information) but their ability to access them is far less than their potential. The only significant institutional change in this area appears to be turning artillery personnel into military police. Collection and analysis in this kind of environment requires very specialized technical skills, vastly different equipment, and most importantly increased cognitive skills (education and training) across the force.

Conclusions

First, the institutional perception that the Army has of itself as primarily a fighting force is limiting its ability to dominate in stability type operations. Stability operations are incidental to land combat. They occur simultaneously. Control in stability operations is dependent on collection of information on adversary's systems. Collection is not just to support targeting. It also supports understanding, which in turn supports information operations.

Soldiers perform the vast majority of collection in stability operations and they need training. Some need very special training (i.e. language skills, surveillance skills…) and special equipment (i.e. long-range acoustic sensors). Standoff systems simply do not have the level of access to adversary systems or the level of resolution and fidelity that a ground force provides. Collection is not just the function of an intelligence organization either. Soldiers provide the greatest amount of actionable information in close combat and stability operations.[110] The land force is also the supporting force for collection in stability type operations whether it wants it or

---

109 The actual sources, means and methods of this type of collection and our current ability to perform this are very sensitive. The study was intentionally vague in this area for classification reasons. Nevertheless, one has only to watch the daily news on current operations in Iraq to know that there is a deficiency in our ability to exploit the potentially unlimited access we have to adversary systems.

110 Soldiers reporting their observations steer intelligence collection efforts. Intelligence organizations perform specialized and technical collection but they require information themselves. In close combat and in stability operations this comes from soldiers on the ground.

not. It has a responsibility to perform this function. This is due to its proximity to the adversary and its potentially unbounded access to the adversary's primary systems.

Second, the current interim Distributed Common Ground Station-Army (DCGS-A) effort and some of the efforts with the Analysis Control Element are clear indicators that the Army does not understand network centric warfare. Since, network centric warfare requires arranging the modular components of collection system into configurations that maximize the power of the GIG, the expectation is that the interim DCGS-A effort and the changes in the Analysis Control Element would fall along these lines. Instead of using technology to change the location of people, both are still trying to reduce forward footprint through replacing people with technology.

The biggest constraint to doing this before was that units in garrison did not have any better access to high bandwidth connections than those in the field. The hundreds of millions spent on this effort to-date could have bought a lot of bandwidth, a lot more capability and saved the untold of millions not yet spent to sustain this effort. IDCGS-A does not have any elements added to the high bandwidth portion of the GIG.[111] It does not improve collection. It does not increase the number of interfaces with other knowledge centers. It also does not increase the speed of information between other elements or increase the number or speed of dissemination methods. It does fix problems in stovepipe hardware programs and it does provide the means for this hardware to communicate together on a very small closed network.

Third, the number and variety of aerial collection platforms needs careful examination at the unit of employment level. A signal's intelligence (SIGINT) gap is continuing to grow due to a lack of integration between ground and air SIGINT systems. Arming the Hunter UAV and turning it into a combat platform, significantly reduces its collection time. The Aerial Common Sensor system combines multiple sensors onto a single platform but does not increase the number

111 Some would argue that the GIG is does not exist. However, this is not true. High bandwidth networks connecting intelligence collection and broadcast dissemination capabilities have existed for years. For a fraction of what was spent on the IDCGS-A effort, connecting garrisons with higher bandwidth and equipping them with more workstations could have taken place. Other services, agencies and many Army strategic intelligence organizations have been working in this environment for years.

of platforms. All of these indicate a lack of understanding in the requirements and employment of these systems.

This Aerial Common Sensor system in particular minimizes the fact that each one of the sensors onboard requires different flight profiles to collect and that these work in multiples to get the accuracy needed to steer other collection systems. The aircraft selected raises many questions about how it is going to access low power and fleeting targets. It cannot loiter at the range and distance required to perform persistent collection on those targets that are of greatest interest. This is also a strategic collection platform and flying it from a forward ground station in a GIG architecture is dumbfounding. There is no doubt it can collect a lot of information. Does it have access to the information systems the adversary is protecting? All this extra information requires processors and people to filter it. This type of vacuum approach is not going to work in a forward ground station.

Recommendations

First, the Army needs to move beyond seeing itself as force that moves across the land delivering death and destruction. It needs to see itself as a force that establishes control as well. Unlike the other services, the Army is employed in midst of an adversary that probably does not want it there. The Army has to stabilize and control the environment as the adversary hides within the civilian population. An adversary in this environment has an information advantage. This provides it freedom of action and places the friendly force in a reactive position. A friendly force without collection access to local adversary systems is operating within a fog of ignorance. Highly specialized training and technical equipment capable of accessing the adversary's local systems (Political, Military, Economic, Social, Infrastructure and Information) provides the only means to take that advantage away.

Second, the requirements determination and resource decision-making processes need review.[112] Currently requirements determination for collection systems focuses on single programs. Requirements determination for Army collection systems currently involves a small group of Army individuals. Predominantly this includes those closely associated with legacy programs. The participation must be much broader to create modular capabilities that support joint requirements. It also has to include consideration of both combat and stability operations.

Army Intelligence is a member of a much larger intelligence community and simultaneously a member of a combined arms team at several levels. Supported commanders should be involved in this process as well. There is a need to balance requirements both horizontally and vertically within the constraints of the 'zero sum' resource game. The collection systems from tactical to strategic level are a single system-of-systems and the requirements should reflect full spectrum collection requirements not just combat. Appendix A and B provides concept sketches of how a systems approach to requirements determination and resource decision making might look like.

Third, the organizational, systems and technical architectures of military intelligence units require review to bring them in line with network centric warfare. The interim DCGS-A solution is all about hardware and local networking. It fails to recognize the cognitive skills in the intelligence process, the actual volume of information at different stages of a campaign, or that the power of NCW comes from capabilities residing inside a robustly interoperable network. Just connecting to the high bandwidth portion of the GIG is not good enough it.

---

112 The way the Army divides itself, by Battlefield Operating Systems (BOS), to make resource decisions are problematic. The structure of the requirements determination process and the resource decision-making process are closely related. While this division makes sense for execution of individual programs and individual training, it does not make sense from a systems perspective for planning, programming and budgeting. The Army provides modular capabilities to a joint force and fights as a combined arms team. This requires operational (or systems) perspectives in developing solutions and balancing requirements and resources from strategic to tactical levels. The reform of the Planning Programming and Budgeting System (PPBS) and the TRADOC organizational structure to reflect the interdependence of these systems is long over due. The resource decisions by one BOS affect the resource and planning decisions of another at numerous levels and are at the root of many of imbalances.

Leveraging the power of the NCW requires organic portions of each military intelligence organization, at every level, permanently resident inside the high bandwidth portion of the GIG (with the equipment and highly trained personnel who know how to leverage the power on it). In this concept, each intelligence activity has a fixed site on the fiber portion of GIG. This portion does not deploy but can echelon capabilities forward depending on requirements. Most importantly, it can grow without increasing forward footprint. This growth could occur on the GIG by assigning another military intelligence unit to support it or through the augmentation of reserves from the local area. The idea is to mobilize information not people.

The forward portion is responsible for local collection, reporting, immediate analysis and directing the activities of both halves. The rear portion is responsible for the larger analysis effort, product generation and dissemination of products from both. Remember that the unit on the fiber GIG has real time access to huge quantities of information and access to a wide variety of dissemination means. The forward portion only has the tactical internet. It can also act as a conduit to broadcast large products created in the forward portion.

This is not a new concept but a very old one. This effort dates back at least to World War II and the Army Air Corps. It has always had success for a time but because it was not an organic relationship among the components it did not have institutional support, it never lasted in peacetime when resources where tight. Some DCGS-A literature is very close to this on the surface but it lacks detail to confirm how close. However, when you follow the money (IDCGS-A) and the literature on efforts related to the Analysis Control Element (ACE) there is great ambiguity on where the community is heading. Appendix C provides a concept sketch of possible systems architecture.

Fourth, the training of military intelligence personnel over the last few decades has moved away from training soldiers to make informed decisions about information toward training soldiers to feed machines that display information or make decisions about information. This is a largely a product of a targeting mentality shared by our Air Force brethren. According to

Mellinger, "Air Power is targeting, targeting is intelligence, and intelligence is analyzing the effects of air operations".[113] Substituting the word ground for air sums up the average perspective most have for intelligence collection. This is fine if you are going to engage the enemy in standoff combat operations with precision weapons.

Unfortunately, our soldiers operate within the midst of a thinking adversary while in close combat and during stability operations. For intelligence professionals, collection and analysis in these environments require very specialized technical skills, vastly different equipment, and most importantly cognitive skills that can inform not confuse commanders. The education and training for this collection effort is far greater than what we now provide soldiers in our schools. Having informed personnel making decisions about information is at the heart of full spectrum dominance and network centric warfare. According to Clausewitz, imperfect knowledge "can bring military action to a standstill."[114]

Our technology is forcing the enemy off the battlefield and into jungles, caves, mountains and cities. This makes the collection on them with standoff technology harder. Combining sensors from ground to space onto a single network and reinforcing it with data links will help to isolate them. However, it will still take soldiers on the ground to penetrate the barriers that adversaries place around themselves. These barriers may be physical like a jungle or social as they try to blend in with civilian populations. It takes a trained soldier penetrate both.

The battlefield still requires soldiers who aggressively pursue information when they have none. Our best collection platforms and sensors are still soldiers. We need to equip them with languages, cultural understanding, powers of observation, and technology. According to Schoomaker, "Soldiers remain the centerpiece of our combat systems and formations… We must prepare all our soldiers for the stark realities of the battlefield."[115] Soldiers must continue to risk

---

113 Phillip S. Mellinger, 10 Propositions Regarding Air Power (Maxwell AFB, AL: Air Force History and Museums Program, 1995), 20.

114 Clausewitz, 95.

115 Schoomaker, 7.

their lives to collect information that enables us to defeat our enemies in combat and control any situation. The next figure is a conceptual display of the gap that exists between potential and actual access to threat systems and the need for trained and equipped soldiers to fill it.

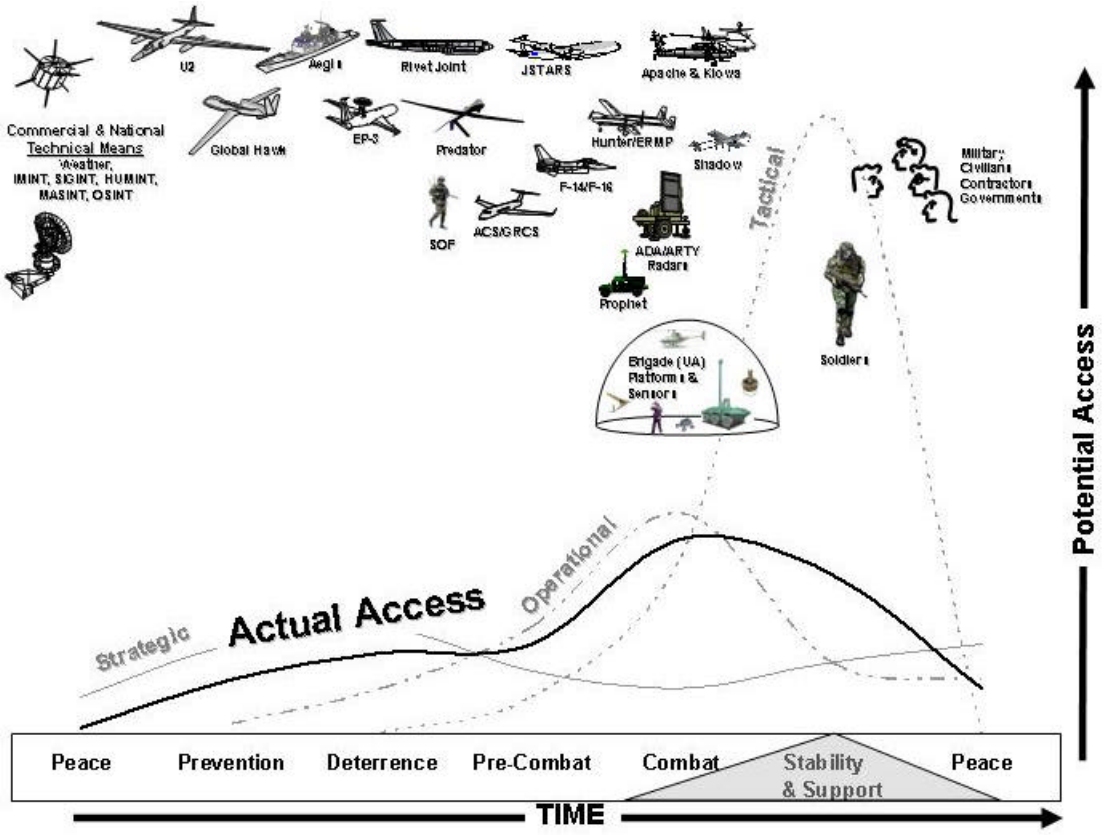
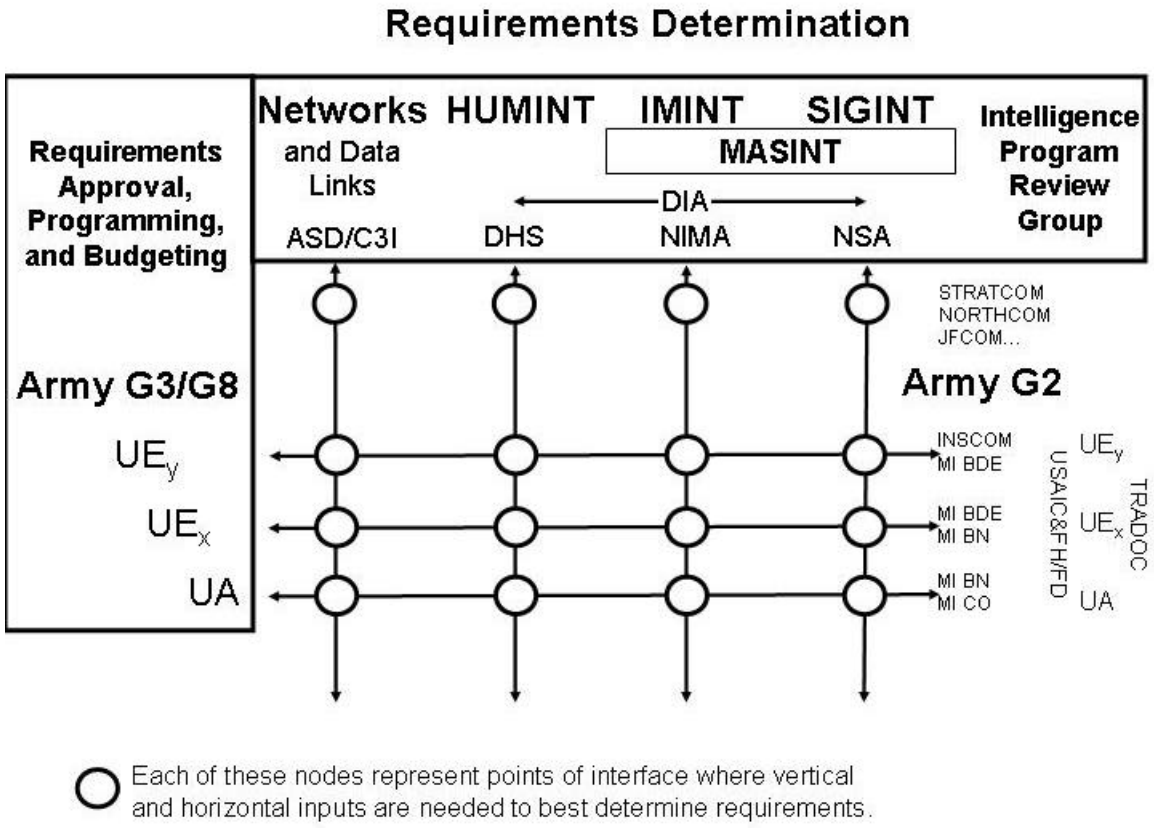


Figure 4, The Gap Between Potential and Actual Access

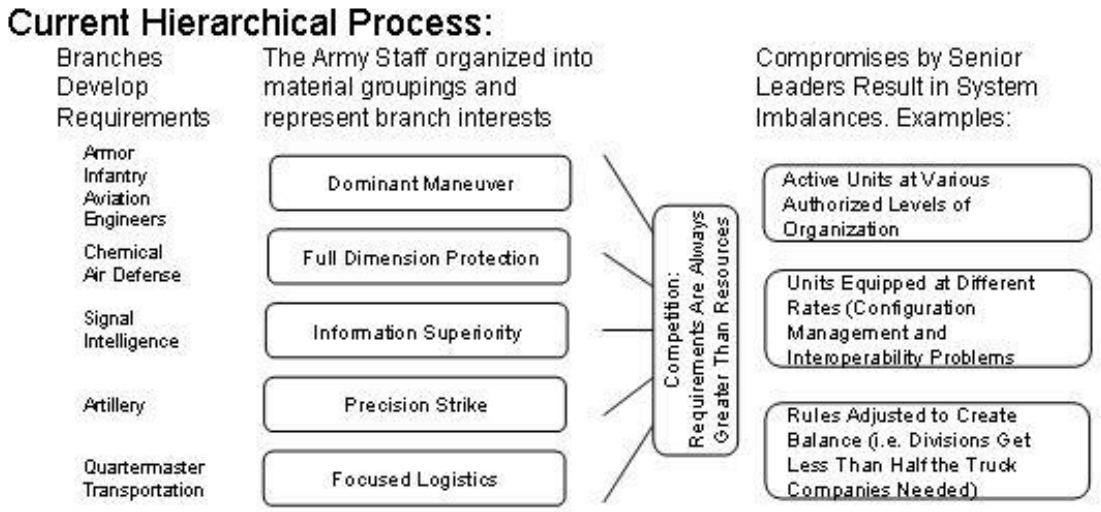
Appendix A

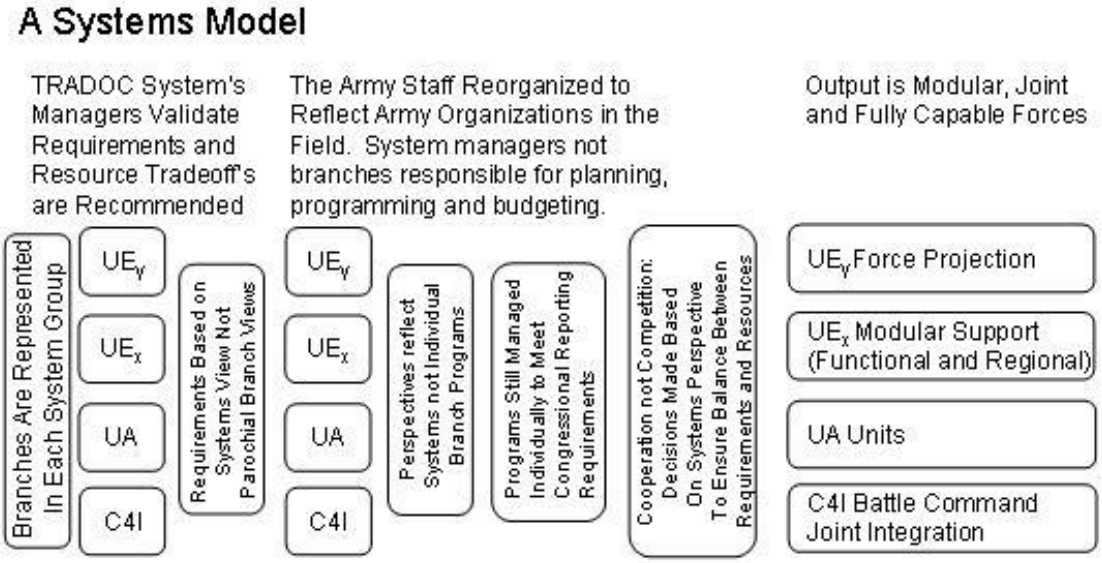
A systems approach to requirements determination for intelligence collection systems and organizations



Appendix B

A systems approach to resource decision making:

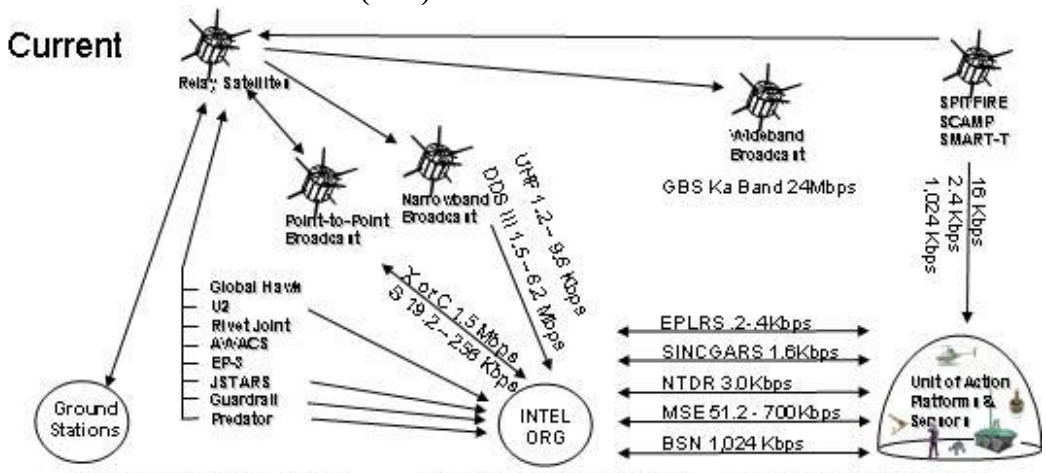




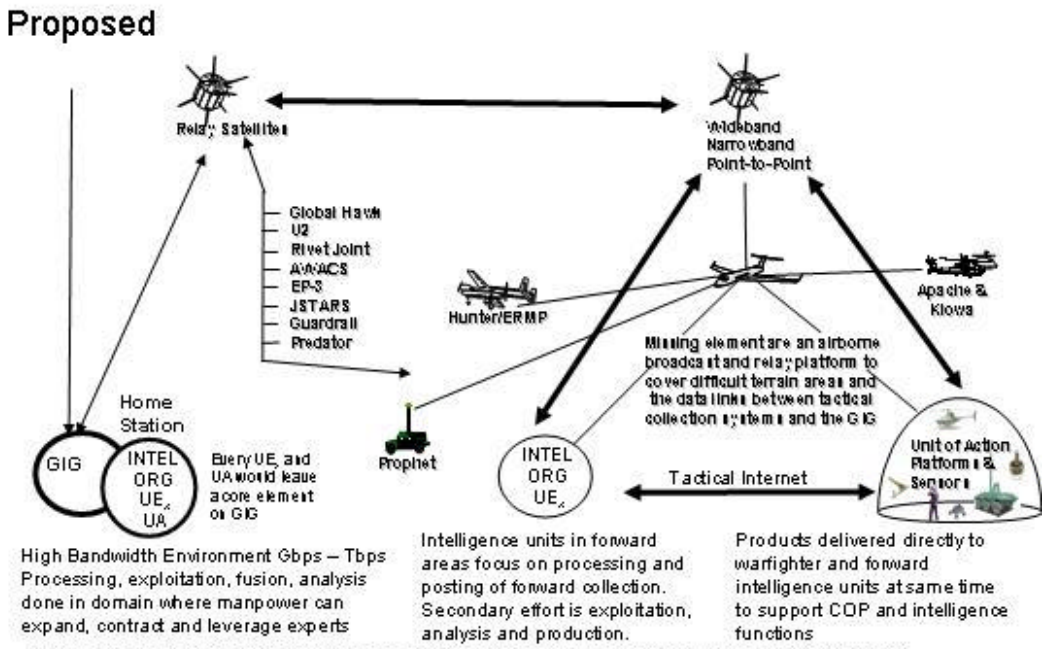
- Institutional army mirrors field army
- Requirements and resource decisions are based on systems perspectives
- Resource tradeoffs recommended and defended by systems managers not branches
- Resource, integration and material management is horizontally and vertically balanced early
- There are eight responsible individuals with incentive to ensure interoperability, balance …
- Zero sum game still exists but now in systems groupings not in branches
- Branches still responsible for execution of individual programs but Planning, Programming and Budgeting would fall under systems managers

Appendix C

Concept sketches of how collection systems and organizations could maximize the power of the Global Information Grid (GIG):



- Architecture ignores cognitive role of humans in process and the ultimate consumer
- A lot of information goes in but little is fully exploited and even less is disseminated



- Maximizes cognitive role in process and leverages full power of network environment
- Missing element in both current and proposed is an airborne platform and data links

Bibliography

Alberts, David S., John J. Garstka and Fredrick P. Stein. Network Centric Warfare: Developing and Leveraging Information Superiority, 2nd Edition (Revised). Vienna, VA: CCRP, 1999.

_____. Understanding Information Age Warfare. Vienna, VA: CCRP, 2001.

_____. Power to the Edge: Command… Control… in the Information Age. Vienna, VA: CCRP, 2003.

Army Security Agency Aerial Reconnaissance: Mission and Sacrifice. Fort Meade, MD: NSA Center for Cryptologic History, 2000.

Bamford, James. Body of Secrets: Anatomy of the Ultra Secret National Security Agency, New York, NY: Anchor Books, April 2002.

Bertalanffy, Ludwig von, General System Theory: Foundations, Development, Applications. New York, NY: George Braziller, 1968.

Brower, J. Michael. "Bandwidth Bonanza," *Military Information Technology*, Volume 7, Issue 10, December 2003/January, 2004 Clausewitz, Carl Von. *On War*. Edited and translated by Michael Howard and Peter Paret. New York, NY: Everyman's Library, 1993.

Crickmore, Paul. *Combat Legend: SR-71 Blackbird*. Shrewsbury, England: Airlife Publishing Ltd., 2002.

Cochran, Alexander S. Jr, et al.,. *Piercing the Fog: Intelligence and Army Air Forces operations in World War II*, ed. John F. Kreis. Washington, DC: Air Force History and Museums Program, 1996.

Codevilla, Angelo. *Informing Statecraft: Intelligence for a New Century*. New York, NY: The Free Press, 1992.

Commander in Chief, Joint Forces Command, *Capstone Requirements Document (CRD): Global Information Grid (GIG)* [document on-line] Washington, DC: Government Printing Office, March 2001, accessed 27 November 2003; available from http://www.dfas.mil/technology/pal/regs/gigcrdflaglevelreview.pdf; Internet.

De Landa, Manuel War in the Age of Intelligent Machines. New York, NY; Urzone Inc., 1991.

Dörner, Dietrich. *Logic of Failure: Recognizing and Avoiding Error in Complex Situations*, trans. Rita and Robert Kimber, Cambridge, MA: Perseus Books, 1996.

DeBlois, Bruce M. "Ascendant Realms: Characteristics of Airpower and Space Power," in *The Paths of Heaven: The Evolution of Air Power Theory by The School of Advanced Airpower Studies*, ed. Colonel Phillip S. Melinger. Maxwell AFB, Ala: Air University Press, 1997..

Fastabend, David A. and Robert H. Simpson. *Adapt or Die: The Imperative for a Culture of Innovation in the United States Army*. Fort Monroe, VA: US Army Training and Doctrine Command, 2003.

Finnegan, John P. *Military Intelligence, Army Lineage Series.* Washington, D.C.: U.S. Government Printing Office, 1998.

Fishel, Edwin C. The Secret War for the Union: The Untold Story of Military Intelligence in the Civil War (Boston, MA: Houghton Mifflin Company, 1996.

Gentry, John A. "Doomed to Fail: America's Blind Faith in Military Technology." *Parameters* XXXII, no. 4 (Winter 2002-03): 88-103.

Gertz, Bill, Breakdown: The Failure of American Intelligence to Defeat Global Terror. New York, NY: Plume, 2003.

Gharajedaghi, Jamshid. *Systems Thinking: Managing Chaos and Complexity*. Boston, MA: Butterworth & Heinmann, 1999.

Hayden, Michael V., Statement for the Record by Lieutenant General Michael V. Hayden, USAF, Director of the National Security Agency/ Chief, Central Security Service Before the Joint Inquiry of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence, 17 October 2002, accessed 21 December 2003; available from http://intellligence.senate.gov/0210hrg/ 021017/hayden.pdf; Internet.

Harvey, LTC Charles, LTC Lance Schultz, "An Analysis of the Impact of Network-Centric Warfare on the Doctrine and Tactics, Techniques and Procedures of Intelligence at the Operational Level," Naval War College Paper, 1 June 1999.

Hurley, Alfred F., William C. Heimdahl, "The Roots of U.S. Military Aviation in *Winged Shield, Winged Sword: A History of the United States Air Force*, vol. 1, *1907-1950*, ed. Bernard C. Nalty. Washington, D.C.: Air Force History and Museums Program, 1997.

Keegan, John. Intelligence in War: Knowledge of the Enemy From Napoleon to Al-Queda. New York, NY: Random House, 2003.

Kipp, Jacob W., Lester W. Grau, "The Fog and Friction of Technology," *Military Review* LXXXI, no. 5. September-October 2001.

Joint Forces Command Glossary, http://www.jfcom.mil/about/glossary.htm, accessed 12 November 2003.

Klein, Gary. *Sources of Power: How People Make Decisions*, Cambridge, MA: The MIT Press, 1998.

Laszlo, Ervin. The Systems View of the World: A Holistic Vision for Our Time. Cresskill, NJ: Hampton Press, Inc., 1996.

Leonard, Robert R. *The Principles of War for the Information Age*. New York, NY: Ballantine Books, 1998.

Mellinger, Phillip S. 10 Propositions Regarding Air Power. Maxwell AFB, AL: Air Force History and Museums Program, 1995.

Melton, H. Keith. *The Ultimate Spy Book*. New York, NY: DK Publishing, 1996.Mitchell, Vance O. "U.S. Air Force Peacetime Airborne Reconnaissance During the Cold War, 1946-1990." In *Golden Legacy Boundless Future: Essays on the United States Air Force and the Rise of Aerospace Power.* Edited by Rebecca H. Cameron and Barbara Wittig. Washington D.C.: US Government Printing Office, 2000.

Mortensen, Daniel R. "The Air Service in the Great War" in *Winged Shield, Winged Sword: A History of the United States Air Force*, vol. 1, *1907-1950*, ed. Bernard C. Nalty. Washington, D.C.: Air Force History and Museums Program, 1997.

Mitchell, Vance O. U.S. Air Force Peacetime Airborne Reconnaissance During the Cold War, 1946-1990. In Golden Legacy, Boundless Future: Essays on the United States Air Force and the Rise of Aerospace Power, ed., Rebecca H. Cameron and Barbara Wittig. Maxwell AFB, Ala.: Air University Press, 2000.

Murray, Williamson and Allen R. Millet. *Military Innovation in the Interwar Period*. New York: Cambridge University Press, 1996.

National Aerial Reconnaissance in the Cold War. Fort Meade, MD: Center for Cryptologic History, 2000.

Naveh, Shimon. In Pursuit of Military Excellence: The Evolution of Operational Theory. Portland, Oregon: Frank Cass Publishers, 1997.

Odom, William E. *Fixing Intelligence for a More Secure America*, New Haven, CT: Yale University Press, 2003.

Peebles, Curtis. *High Frontier: The United States Air Force and the Military Space Program.* Washington, D.C.: U.S. Government Printing Office, 1997.

Richelson, Jeffrey T. *The U.S. Intelligence Community, Fourth Edition.* Boulder, Colorado: Westview Press, 1999.

_____. The Wizards of Langley: Inside the CIA's Directorate of Science and Technology. Cambridge MA: Westview Press, 2001.

Sontag, Sherry., Christopher Drew and Annette L. Drew, *Blind Man's Bluff: The Untold Story of American Submarine Espionage*. New York, NY: Harper Paperbacks, 1998.

Schoomaker, Peter J. Gen, CSA. The Way Ahead: Our Army at War ... Relevant and Ready. Moving from the Current Force to the Future Force …Now! Washington, DC: Army Strategic Communications, November 2003.

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

Smith, Edward A. Effects Based Operations: *Applying Network Centric Warfare in Peace, Crisis, and War.* Vienna, VA: CCRP, 2002.

Tzu, Sun. *The Art Of War*, trans. Samuel B. Griffith. New York, NY: Oxford University Press, 1963.

U.S. Department of the Army, *FM 3-0: Operations.* Washington, D.C.: US Government Printing Office, 2001).

_____. *How the Army Runs: A Senior Leader Reference Handbook.* Washington, D.C.: Government Printing Press, 2001.

_____. *Army Intelligence Transformation Campaign Plan (AI-TCP)*, Washington, D.C.: Deputy Chief of Staff for Intelligence, 2003.

_____. *System Training Plan for the Distributed Common Ground Station – Army*, Ft Huachuca, AZ: United States Army Intelligence Center, 2003.

U.S. Department of Defense, Joint Publication (JP) 1-02: Department of Defense Dictionary of Military and Associated Terms. Washington, D.C.: US Government Printing Office, 2000.

_____. Joint Publication (JP) 2-0: Doctrine for Intelligence Support to Joint Operations. Washington, D.C.: US Government Printing Office, 2000.

_____. *Network Centric Warfare: Department of Defense Report to Congress* [document on-line] Washington, DC; Government Printing Office, 27 July 2001, accessed 24 October 2003; available from http://www.dod.mil/nii/ncw; Internet.

Witsken, Jeffrey R. "Integrating Tactical UAVs Into Armor and Cavalry Operations." Armor Magazine (March-April 2003.