



**STRATEGY
RESEARCH
PROJECT**

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

**DISTRIBUTED COLLABORATIVE ANALYSIS:
A NEW APPROACH FOR INTELLIGENCE ANALYSIS**

BY

**LIEUTENANT COLONEL GUS E. GREENE, Sr.
United States Army**

**DISTRIBUTION STATEMENT A:
Approved for Public Release.
Distribution is Unlimited.**

USAWC CLASS OF 2001



U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

20010605 213

USAWC STRATEGY RESEARCH PROJECT

Distributed Collaborative Analysis: A New Approach for Intelligence Analysis

by

Gus E. Greene Sr.
United States Army

Professor Tony Williams
Project Advisor

The views expressed in this academic research paper are those of the author and do not necessarily reflect the official policy or position of the U.S. Government, the Department of Defense, or any of its agencies.

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

DISTRIBUTION STATEMENT A:
Approved for public release.
Distribution is unlimited.

ABSTRACT

AUTHOR: Gus E. Greene Sr.
TITLE: Distributed Collaborative Analysis: A New Approach for Intelligence Analysis
FORMAT: Strategy Research Project
DATE: 10 April 2001 PAGES: 44 CLASSIFICATION: Unclassified

In the post Cold War environment, the threats to our National Security have grown more complex, dynamic, and uncertain. To further add to the complexity of the environment, the rapid growth in information age technologies continues to compress the dimensions of time and space significantly, while seeming to justify calls for resource reductions by the public. At the same time, the rapid pace of this growth has caused decisionmakers at all echelons - tactical to strategic - to challenge the Intelligence Community to become more responsive and agile in meeting their demands for intelligence. These strategic trends demand an Intelligence Community that can dominate the full spectrum of economic, political and military intelligence.

Today's Intelligence Community, which evolved out of the necessity to contend with wars and technology, is a hierarchical structure that cannot compete in the information age. Recent advances in both the business and military intelligence communities indicate that success demands a change. One such change is to embrace a new method for analysis that is collaborative and distributed, facilitated by the Internet and its associated technologies. Although this approach requires improvements in interoperability of systems, security and a major cultural change within the Intelligence Community, doing so will significantly enhance its ability to deal with the effects of a more complex, dynamic and uncertain world, the information age, and the impact of limited resources.

TABLE OF CONTENTS

ABSTRACT	iii
PREFACE.....	vii
DISTRIBUTED COLLABORATIVE ANALYSIS: A NEW APPROACH FOR INTELLIGENCE ANALYSIS ..	1
INTELLIGENCE ANALYSIS - A DEFINITION	2
ORIGINS OF THE HEIRARCHICAL INTELLIGENCE STRUCTURE	3
The First Intelligence Analysis Organizations	4
World War I.....	5
World War II.....	5
The Cold War.....	6
The Intelligence Community of Today	6
Why a Redundant Analytical Structure?.....	7
THE CHALLENGES IN TODAY’S INFORMATION AGE ENVIRONMENT	8
Expansion of the Subject Matter	8
Growth of Information Technologies.....	9
The Lack of Governmental Support for Intelligence at Any Cost	9
The Compression of Strategic and Tactical Information Domains	10
BUSINESS SOLUTIONS TO ANALYSIS	10
Virtual Workspace.....	11
LESSONS FROM THE TACTICAL FORCE – TRANSFORMATION OF ARMY INTELLIGENCE	12
Virtual Analytic Control Element (ACE)	15
DISTRIBUTED COLLABORATIVE ANALYSIS – A NEW APPROACH FOR THE COMMUNITY.....	17
THE CHALLENGES TO ACHIEVING DISTRIBUTED COLLABORATIVE ANALYSIS.....	20
CONCLUSION.....	22
ENDNOTES	25
BIBLIOGRAPHY	29

PREFACE

Throughout life, I have sought to determine how things worked. Unfortunately, I often broke things in the process. However, I always learned from the experience and attempted to use the knowledge that I gained to improve. I owe a huge debt to my patient and loving parents who suffered through those early inquisitive years where I nearly lost a thumb blowing up my chemistry set and nearly burned the house down in a separate incident. Despite these events, they have continued to support my, sometimes dangerous, quest for knowledge.

I also owe a tremendous debt to my wife and friend who helped me weather the college years, which brought about my interest in technology and computers. Her support has continued throughout my military career, where the quest for knowledge about the world of intelligence began. This paper is a continuation of that quest.

LIST OF ILLUSTRATIONS

FIGURE 1 – THE “VIRTUAL ACE” 16

DISTRIBUTED COLLABORATIVE ANALYSIS: A NEW APPROACH FOR INTELLIGENCE ANALYSIS

“ You must keep pace with developments in a tremendously complex society which, ... gropes for answers to challenges its founding fathers could never have conceived.”

- President Lyndon B. Johnson, 18 September 1967

In the post Cold War environment, the threats to our National Security have grown more complex, dynamic, and uncertain. Aggressive and coercive state and non-state actors threaten regional stability. The spread of dangerous technologies and weapons of mass destruction pose an increasing menace to society as a whole. Further, some failed and failing states are creating events that may require the United States to employ its national power to alleviate suffering, enforce human rights or halt violence.¹ These events significantly challenge the Intelligence Community (IC) to deal with a broader spectrum of potential threats than during the Cold War period.

To further add to the complexity of the environment, the rapid growth in information age technologies continues its impact. The Internet, as it evolved from the Advanced Research Project Agency (ARPA)-net, has been embraced around the globe as a means of human communication via computer. This new environment created a “cyber-space” for interaction, communication, and information.² As a result, information age technology has significantly compressed the dimensions of time and space, while facilitating organizational downsizing.

These strategic trends demand an Intelligence Community that can dominate the full spectrum of economic, political and military intelligence. The rapid pace of growth in information age technologies has caused decisionmakers at all echelons - tactical to strategic – to challenge the Intelligence Community to become more responsive and agile in meeting their demands for intelligence. To achieve this end, the community must divest itself of Cold War analog methods of analysis within its limited hierarchical structure. Success demands a change. One such change is to embrace a new method for analysis that is collaborative and distributed, and uses automation and the technologies inherent in the Internet to significantly enhance the Intelligence Community's ability to deal with these challenges while overcoming the effects of downsizing.

INTELLIGENCE ANALYSIS - A DEFINITION

Intelligence is the product that results from the collection, processing, exploitation, integration, and analysis of available information concerning foreign countries or areas.³ This information can come from many sources that are both covert and overt. An expert, or a group of experts, gathers data or information to make informed assessments as to relevance and reliability. These experts then either consolidate the information into some form that is usable by decisionmakers or make informed assessments as to a future condition that will require decisions. In fact, most businesses today perform very similar tasks to gain an advantage over others that compete in their particular endeavor. The business community now commonly refers to this as business intelligence. The business community uses a set of concepts, methods, and processes along with information from multiple sources. It then applies experience and assumptions to develop an accurate understanding of business dynamics and improve business decisions. It involves gathering, management, and analysis of data to produce information that is then distributed to people throughout the organization to improve strategic and tactical business decisions.⁴ Therefore, from a general perspective, the activities used to produce intelligence are not unique to the intelligence community and analyzing other approaches may help us solve similar problems in the Intelligence Community.

What makes the United States Intelligence Community unique from its business intelligence counterpart is twofold. First, there is a requirement to conduct both covert and highly technical information gathering activities. Any compromise of these activities and capabilities may lead to an increased investment in technical collection to make up for the compromise or it may lead to the complete loss of the information or the source. Worse, compromise may prove to be politically damaging to the nation. Therefore, the intelligence community deals with this problem by classifying the information to protect the ability to continue to have access, to protect the source and protect National Interests. The obvious drawback is that classifying information also limits its availability to a select few.

The second element that makes the intelligence community unique is the scope of the analytic problem. Unlike its business community counterpart that focuses on a much narrower information set, the intelligence community performs analysis of both classified information and unclassified information across multiple disciplines (HUMINT, SIGINT, PHOTOINT, MASINT) and across multiple domains (political, economic, informational, and military). Its goal is to produce a perspective on the current situation and predict possible future activities or circumstances that facilitate the decisions of both senior military and political leaders alike.

For the intelligence community, then, analysis is the process of transforming the bits and pieces of both classified and unclassified information that are collected by numerous sources into something that is usable by policy makers and military commanders.⁵ The intelligence community divides intelligence analysis into two very broad categories – technical analysis and all-source analysis.

Technical analysis as defined by Abram Shulsky is the body of “analytic methods that transform highly specialized data, totally or virtually incomprehensible to everyone but a specialist, into data that other intelligence analysts can use.” Examples include cryptanalysis or code breaking, telemetry analysis or the study of missile radio signals, and photo interpretation.⁶ As more sophisticated forms of collection are developed, experts will form new methods of technical intelligence analysis as well. An example of this is in the relatively new discipline of Measurement and Signatures Intelligence (MASINT) and the analysis of multi-spectral imagery. These specialized forms of analysis can result in a finished intelligence product by themselves but more often are keys to performing all-source Intelligence.

The term, “all-source Intelligence” is used to describe the products, organizations and activities that incorporate “all sources” of information including human intelligence, signals intelligence, imagery intelligence, measurement and signatures intelligence, and open source information in the production of finished intelligence.⁷ It also encompasses the political, economic, and military information domains as well. Thus, “all-source analysis” is the process used to produce “all-source intelligence.” It encompasses the myriad of tasks associated with gathering of classified and unclassified information from multiple echelons, sources and disciplines and transforming it into something that is usable by policy makers and military commanders to meet their needs. The finished intelligence product might be a simple statement of facts, an evaluation of the capabilities of another nation’s military forces, or a projection of a likely course of political events in another nation.⁸ This definition of all-source analysis is important because it implies a need for information sharing that is not as pervasive as one would hope for. It is here that the community can derive the greatest benefit from embracing a new method for conducting analysis.

ORIGINS OF THE HEIRARCHICAL INTELLIGENCE STRUCTURE

The United States Intelligence Community has a very short history, but has its roots in the beginning of our Nation where General George Washington personally directed the Continental Army’s intelligence service, running a number of highly successful intelligence operations.⁹ In

tracing the development of the intelligence community, it can be seen that war and technological advancements have resulted in a hierarchical analytic structure that supports the unique needs of decisionmakers at every echelon.

THE FIRST INTELLIGENCE ANALYSIS ORGANIZATIONS

In the nineteenth century, analysis was highly centralized. It was predominantly conducted in the mind of the Military Commander. Scouts and other sources reported directly to the commander who performed his own assessment of the situation. This changed as information gathering capabilities grew more complex and the volume of information expanded. Agents, scouts, and cavalry units brought increasing amounts of information that needed to be filtered, sorted and assessed. New technologies such as the telegraph and telephone not only dramatically changed the nature of communications, they also added to the complexity of the information environment and thus the analytic problem. Up until then, couriers, postal services, and diplomatic bags represented the major means of communications although visual signals such as semaphore flags, or heliograph mirrors were used as well.¹⁰ With the increases in information brought about by new technology and added capabilities, intelligence analysis organizations developed that were small, ad hoc and predominantly limited to Military Intelligence activities. During the Civil War, for example, the Army of the Potomac established the Bureau of Information to collate reports sent back from agents, scouts, and cavalry patrols with information from prisoners, and deserters. New technologies such as observation balloons and new techniques such as tapping of telegraph lines were used as well¹¹

By the 1880's, urbanization, industrialization and technological advances had a dramatic impact on the way people lived, and with it, set the stage for the way in which intelligence would be organized and how analysis would be performed.¹² This period of change resulted in the first permanent intelligence organizations devoted to the management of collection activities and analysis of collected information. The Office of Naval Intelligence was born in 1881 to "collect and record such naval information as may be useful to the department in wartime as well as in peace."¹³ The Military Information Division of the Adjutant General in 1885 was established to collect "military data on our own and foreign services which would be available for use by the War Department and the Army at large."¹⁴ As the fledgling beginnings of the hierarchical intelligence structure began to take shape, new technologies continued to appear. In 1881, Marconi's wireless communications as well as the Wright Brother's first flight set the technological pre-conditions for the future of intelligence analysis organizations. It was these

technologies and the outbreak of the Great War that saw the biggest expansion in the need for additional technical, and all-source analytic organizations to handle the expanding information environment.

WORLD WAR I

America's entry into WWI established a need for fused all-source intelligence. The re-establishment of the Military Intelligence Section of the War Department General Staff satisfied it and added to the structure of intelligence. This organization was originally established following the Spanish American War but was dissolved in the post war reductions that followed.¹⁵

Technological advancements in Marconi's wireless communications and Russian success in communications intelligence (COMINT) brought about the development of a specialized cryptanalysis element known as MI-8 as a sub-section to the War Department's Military Intelligence Section.¹⁶ This brought into existence the first COMINT capability in the United States Army. Intelligence also capitalized on the Wright Brother's air exploits to provide both visual and photographic coverage of enemy positions. Photo analysis as a discipline was thus born and added to the military structure.¹⁷ The Army also collected human intelligence (HUMINT) through both traditional and non-traditional (covert) means.¹⁸ Advancements in technology and World War brought about the existence of the intelligence disciplines as well as the beginnings of the technical analysis that we have today.

WORLD WAR II

By the mid-twentieth century, the United States Intelligence Community began to add structure to the hierarchy to achieve a national level assessment. World War II and the need for national level information led to the expansion of intelligence capabilities beyond the small and compartmented Defense (Naval and Army) Intelligence Community.¹⁹ In 1941, the Coordinator of Information was established which later became the Office of Strategic Services (OSS) in 1942.²⁰ With the establishment of this office, the national intelligence community and an associated intelligence analytic capability was born. As the scope and complexity of the information environment grew, the OSS grew as well. It rapidly became a sophisticated research and analysis organization, providing strategically relevant military, atomic research, and weapons information, as well as providing intelligence collection in support of Allied troops.²¹

THE COLD WAR

With the end of World War II, and the onset of the Cold War, more changes occurred in the development of the modern intelligence analytic community. The Cold War was a war of ideology that the United States and its Allies fought ferociously in the intelligence domain. The fact that the Soviet Union and its "Iron Curtain" was largely a closed target, forced the U.S. to resort to a variety of largely remote technical systems to collect required intelligence and access Soviet capabilities.²² As a result, the intelligence community formed new technical analysis organizations to capitalize on new technologies and the expanding need for information about the Cold War threat. With this expansion came the problem of coordinating a common position among the various intelligence organizations. Conflicting information and assessments from the various stove-piped intelligence organizations demanded a mechanism for supporting the national level with an all-source assessment of the political, economic, and military information associated with the Cold War threats.

The National Security Act of 1947 brought about the most dramatic change to the Intelligence Community as it provided a legal basis for its existence, and formed the Central Intelligence Agency, to coordinate and evaluate the intelligence produced by other departments (such as the Department of Defense) in a single unified assessment.²³

THE INTELLIGENCE COMMUNITY OF TODAY

Today's Intelligence Community grew out of the Cold War into a complex group of organizations predominately designed to support the hierarchical decisionmaking structure of the government.²⁴ It includes the Central Intelligence Agency (CIA), the Department of Defense intelligence organizations that support the national level (the National Security Agency, the National Reconnaissance Office, and the National Imagery and Mapping Agency), the service Intelligence organizations and those elements supporting the intelligence components of the unified commands. Finally, the community includes the Departmental intelligence organizations made up of the Defense Intelligence Agency, the Department of State's Bureau of Intelligence and Research, the Department of Energy, the Department of the Treasury and the Federal Bureau of Investigation.

As the previous history suggests, the community was formed out of necessity not planning. War and technological advancements were the catalysts, rather than efficiency. The Community's general organization resulted from two specific needs. One was to support the

hierarchical decisionmaking structure within the government. The other was to provide the analysis of the information derived from technical or unique sources. For example, the CIA's analytic efforts support the President, the State Department's Bureau of Intelligence and Research supports the Secretary of State, the Defense Intelligence Agency supports the Department of Defense's unique military information needs, and the field commander is supported by the service intelligence organizations.

Organizations such as NSA and NIMA, on the other hand, perform technical analysis and support the development of finished intelligence by the rest of the community. Although much information sharing exists today, the community can still be described as a group of stovepiped information channels that are divided by intelligence discipline (SIGINT, IMINT, HUMINT, MASINT) and further divided by level within the hierarchy (Strategic, Operational, and Tactical), some with overlapping functions.

At the national level, for example, the CIA's Directorate of Intelligence, the State Department's Bureau of Intelligence and Research, and the Defense Intelligence Agency perform all-source analysis and have functions that overlap. They have access to the full range of collected intelligence and each works virtually on the same issues.²⁵ Although narrower in scope to geographic areas of responsibility, the military intelligence capabilities of the services and the supported Commanders in Chief (CINCs) also have functions that overlap as well.

WHY A REDUNDANT ANALYTICAL STRUCTURE?

It is easy to see why we have specific analytic organizations that perform technical analysis on the various types of collection (imagery, signals, espionage). The technical nature of the information demands analysts with unique skills to transform the collected information into a usable product. It is less obvious why we need to have a redundant all-source analytic structure. The reasons for creating the agencies and organizations that perform all-source analysis with functions that appear to overlap, even though each works on virtually the same issues, are consumer needs and the idea of competitive analysis.²⁶

First, senior leaders/policy makers (the President, the Secretary of Defense, the Secretary of State, the Chairman of the Joint Chiefs of Staff, as well as the CINCs and subordinate commanders) have very different intelligence needs. Even when working on the same issue, each one has different responsibilities that require different information. All, however, require some measure of political, economic, and military information but at a different fidelity and scope. Thus, the U.S. developed analytical centers to serve these unique needs. Admittedly,

each desires an assured stream of intelligence dedicated to those needs.²⁷ The basic requirement is to have sufficient intelligence resources to provide tailored products that meet the needs of the decisionmakers.

A second reason for developing multiple organizations with overlapping functions deals with the idea of competitive analysis. The fundamental concept is to have several agencies, with differing backgrounds and views, perform analysis on an issue to gain a greater depth of appreciation of the problem's many facets. The unique expertise of those involved allows for a more varied approach and multiple points of view to be considered. Thus, the group tends to eliminate parochial views and achieves a closer "proximate reality" of the analyzed situation. It also appears to be an effective antidote to "group think."²⁸

Clearly, senior leaders throughout the hierarchy have specific information needs that are unique to their decisionmaking. Thus, each requires access to experts that have knowledge of their requirements and can construct tailored products to support their information needs. The problem with the recent efforts to downsize and centralize analysis is that there are fewer and fewer resources available to meet the expanding information needs of the dynamic and fluid environment. Competition for resources, the hierarchical need for experienced analysts familiar with the each organization's information requirements, and the competitive analytic approach demand that each level have equivalent if not the same analytic capability. This hierarchical structure with its stove piped information flow means that the intelligence community has a reduced ability to leverage the analytic capabilities of the entire nation and is risking its ability to compete in the post cold war information age environment.

THE CHALLENGES IN TODAY'S INFORMATION AGE ENVIRONMENT

In this post-Cold War environment, four emerging trends further complicate the intelligence analytic challenge. These trends include the expansion of the subject matter from a Soviet centric model, the growth of information technologies, the lack of governmental support for intelligence at any cost²⁹ and the compression of strategic and tactical information domains.

EXPANSION OF THE SUBJECT MATTER

During the Cold War, the threat was somewhat clearer and more distinct. The single strategic threat from the Soviet Union provided a remarkably stable intelligence target.³⁰ This stable target gave sharp focus for both collection and analysis. The fall of the Soviet Union has

changed those conditions. The problem faced by intelligence analysts is significantly more diverse, and broader in scope, making all-source analysis more important and relevant.

Today the threats to US interests involve ethnic, religious, and economic threats that include more than one country or issue. Grappling with them requires a broad array of expertise that is seldom found in one place. US military deployments to Bosnia, Haiti, Somalia, and other areas where the US military has little or no previous knowledge or experience underline the need for global analytic coverage.³¹ Yet, even today, poor communications and coordination exists between the intelligence services and the executive departments.³² For example, while the U.S. Army, as the Department of Defense executive agent, is charged with producing scientific, technical, and general military intelligence on foreign ground forces, this material has limited circulation in the national community.³³

GROWTH OF INFORMATION TECHNOLOGIES

In addition to the complexity associated with an expanding array of threats, the changes in information technologies have also compounded the analytic problem. The huge growth in information technologies and reduction in cost means that more information is readily available and can be had faster than ever before. As John Gannon, Chairman of the National Intelligence Council points out, "Information abounds. A lot of open source material is relevant to our needs. Everybody is better informed. Intelligence requirements, as a result, tend to be sharper and more time sensitive. Everything moves faster."³⁴ The resulting compression of time and space has forced decisionmakers to demand finished intelligence more rapidly than ever before.

This growth in information technologies is a two edged sword. On the one hand, it demands increased technical capability to collect and analyze the myriad new sources for intelligence. On the other, it demands that the Intelligence Community keep pace with new technological advancements so that it does not lose its competitive advantage to a potential threat.

THE LACK OF GOVERNMENTAL SUPPORT FOR INTELLIGENCE AT ANY COST

In this post-Cold War environment, the change in domestic politics calls for a more cost effective approach to intelligence than in the past. During the Cold War, the closed nature of the Soviet society, and the dual threats of communist imperialism and Soviet strategic nuclear weapons, justified the size of the intelligence budget. In fact, it was easy to justify expansion. With the demise of the Soviet Union, not only did the arguments for spending more die with it,

the current budget has come under increasing scrutiny as well. The government is no longer supportive of the idea of "intelligence at any cost." As a result, Congress has charged the community to find ways to share resources, be more efficient and effective, reduce overhead, and to downsize³⁵

THE COMPRESSION OF STRATEGIC AND TACTICAL INFORMATION DOMAINS

Finally, the post-Cold War environment finds the United States increasingly involved in Operations other than War (OOTW) that blur the traditional strategic, operational and tactical intelligence boundaries that have previously defined relationships between intelligence organizations. An example is in Operation Joint Endeavor (Bosnia). Military Intelligence personnel supporting the consumers at the tactical level, in order to be effective in analyzing intentions and conducting predictive analysis, had to understand the objectives underlying the conflict and project how the factions would continue to seek "victory" using non-military strategies. This required an understanding of the political objectives of the belligerents, a domain in which military intelligence professionals at the tactical level have little experience and training.³⁶

This blurring of the intelligence boundaries calls for greater transparency within the community that facilitates the free flow of information. The fact that an act by a single American soldier in a foreign country can now have strategic implications indicates that there must be greater interaction and collaboration between echelons.

Ultimately, the purpose of analysis is to minimize uncertainty, make sense of complex issues, and call attention to emerging problems or threats.³⁷ Given recent trends in the post-Cold War environment, we cannot rely on the centralized hierarchical approaches of the past to achieve these ends. In this information age, rather than reorganizing and further centralizing functions to facilitate information sharing and collaboration, we can mitigate the effects of time and space compression, reductions of personnel, expansion of the global information environment, and achieve synergy by bringing these distributed nodes of analysis together into a virtual network of analytic power.

BUSINESS SOLUTIONS TO ANALYSIS

An example of this approach can be found in the automated business community concept known as a Cooperative Distributed Problem solving system (CDPS). CDPS is a distributed network of semi-autonomous processing nodes that work together to solve a set of inter-related

problems. Each node is a sophisticated problem-solving system that can modify its behavior as circumstances change, and can plan its own communications and cooperation strategies with other nodes as the situation dictates.³⁸ The idea behind the CDPS approach is that there is an advantage to distributing the problem solving process.³⁹ Rather than the linear process of collecting, processing, analyzing, and disseminating intelligence, as in our current intelligence analysis model, CDPS holds that the solution to the overall problem can be distributed. It divides the solution of the analytic problem into subsets that relate to the whole. Thus, many problems related to the broader problem set can be solved simultaneously. It, therefore, improves the speed with which the problem is solved, since parallel activities occur simultaneously.

It also mitigates considerations of bounded rationality, a principle of human reasoning formulated by Herbert Simon (1957) that states that the capacity of the human mind for formulating and solving complex problems is small compared with the size of the problems that need to be solved for objectively rational behavior in the world. Put simply, real problems are simply too big for a single program or single thread of control to solve. A single intelligence organization, for example, cannot possibly meet all of the information requirements of the entire Intelligence Community. There are too many different kinds of knowledge that need to be applied and too many different decisions that need to be made too quickly to accomplish complex problem solving in a centralized manner.⁴⁰ The expanded scope of the intelligence problem, the rapid growth in technology, the compression of the Strategic to Tactical information domains and governmental demands for improved efficiency, all argue that the Intelligence Community must be more distributed, networked and collaborative. This approach requires more transparency between organizations, rather than centralization of functions and control. Centralization and linear processes cannot achieve the efficiencies that are needed to satisfy simultaneously the unique needs of the entire Intelligence Community at the appropriate fidelity and scope.

VIRTUAL WORKSPACE

Another trend in the business community that can facilitate the idea of CDPS is virtual workspaces. More and more large corporations are taking advantage of telecommuting and virtual office techniques that convert the centralized, rigid, hierarchical office workspaces into flexible interactive office environments characteristic of a virtual organization. Organizations that have employed this idea have increased productivity, lowered costs, and bolstered

employee satisfaction. These models of organizational structure take advantage of the flexibility offered by information age technology. They allow rapid teaming of groups in order to meet specific organizational needs and compensate for the rigid centralized hierarchical structures of the past without physical reorganization. The flexible, virtualized organizations benefit by their ability to physically locate closer to customers and tie into customer needs, while achieving greater efficiency in employing corporate intellectual assets. This method significantly improves the ability to leverage the specialized knowledge within and across organizational boundaries without physical collocation or centralization.⁴¹

With the advent of the Internet, new technologies abound that facilitate collaboration between distributed elements in these virtual organizations. Today, software is available that provides a unique collaborative computing environment that mimics an office environment. The computer becomes a virtual space where applications, documents, and people are directly accessible by people in virtual rooms, floors, and buildings no matter where they physically reside. For the user, each room provides a place to communicate and share information no matter what the form. In other words, people can gather in "rooms" to talk, using desktop audio/video conferencing. They can share text, data, and information and collaborate using shared whiteboards, facilitated by the "John Madden Pen" capability that has become popular in assisting T.V. viewers' understanding during replays on Monday Night Football. URLs, notes and other documents or data can be shared via the users' local applications (word processors and graphics programs, etc). These technologies can now serve to eliminate the physical boundaries inherent in industrial age institutions, but it requires leadership to overcome the cultural boundaries required to make the shift to a new way of doing business.

LESSONS FROM THE TACTICAL FORCE – TRANSFORMATION OF ARMY INTELLIGENCE

An example, which may be helpful in understanding the application of these business practices, can be found in the Army's efforts to digitize the force. Recently, the Army embarked upon a campaign to transform itself into a force that is capable of dominating across the entire spectrum of operations from peacetime engagement activities, deterrence and, if required, to full scale war.⁴² Fundamental to the transformation strategy is the requirement for enhanced situational awareness to mitigate the impacts of making the force lighter and more deployable.

The increased speed and pace of maneuver have created an environment where commanders must see farther and think faster with ever increasing precision. This situation is not much different than that faced by the broader Intelligence Community. Technology has added to this challenge by providing a wealth of information, not all of which is relevant.⁴³

Joint Vision 2010 defines the challenge to the Military Intelligence Community of the future. It must be capable of providing complete situational understanding, battlespace visualization, and information superiority through collaborative, interactive, integrated, and interoperable intelligence databases and networks.⁴⁴ In other words, to leverage the idea of cooperative distributed problem solving, using a virtual workspace in a networked environment. Army Intelligence took its first step towards this goal during the Division-level Advanced War Fighting Experiment (AWE) conducted at Fort Hood, Texas in 1997.

Much like the larger national Intelligence Community, the Army intelligence community is hierarchical. Each headquarters has an analytic element devoted to the analysis of information. The reasons for the redundant and overlapping capabilities are the same as those of the national community. The intelligence needs at each echelon of command are unique and must be tailored to meet the decisionmakers' requirements. Additionally, each echelon has its own dedicated collection capabilities that demand an independent analytic capability.

The AWE fundamentally changed the way that intelligence was produced within the Army. In the past, each echelon would receive reports from its organic collection capabilities, process and analyze this information into both a current assessment of the situation and an assessment of future threat activities independent of the analysis conducted by others throughout the hierarchy. The major limiting factor to distributing analysis and collaborating on results was communications. Since analysts at the higher headquarters could not share data or analysis between echelons in a timely fashion, the resulting assessments were often irrelevant to subordinate commander's information needs. Conversely, communications limitations also constrained the timeliness of reporting from subordinate units. This meant that higher echelons of command had to re-analyze the reported information to assess the impact of activities that had transpired since the time of the original report. Thus, intelligence assessments at every echelon were complicated by having to re-evaluate outdated information in order to understand the current situation, and build assumptions about the future. In essence, the inability to share information and analysis in real time meant that every echelon in the hierarchy defaulted to performing analysis locally to meet the supported headquarters' information needs, often disregarding the assessments of subordinate and higher commands.

The AWE introduced the Army to the Internet, which significantly changed the way that intelligence was performed. With the added improvements in communications, there was an idea that reorganization of the intelligence structure into a more centralized structure could be more efficient. Some believed that it would be possible to consolidate and perhaps reduce intelligence resources in order to provide an all-source analytic product that supported all subordinate echelons of command. Through numerous training exercises, the leadership determined that this solution was not practical. No single processor or analytic organization had the capacity to analyze every bit of data, and report from every collector, sensor, and analyst on the battlefield to provide tailored products that would support the needs of all subordinate and supporting headquarters and commanders' unique information needs. The management of the task was overwhelming. Even with the improved capacity, the existing tactical communications precluded sending every report to a central location without a serious backlog. Even if we could get the information to a central location, the ability of analysts to rapidly sift through the volumes of data and produce a relevant picture and assessment for the myriad of different consumers was an insurmountable task for a single organization. The risk of a single point of failure was also a practical reality that was not worth taking. Finally, commanders were concerned about losing their dedicated intelligence support and the intelligence team was concerned about losing the close relationship that had been fostered that assists in assuring that the right information is developed to meet the commands needs. In the final analysis, it was determined that a sufficient number of analysts must work directly for the consumer (the commander) and be habitually associated with the organization on a permanent basis to understand the consumer's information requirements. Since, the total number of personnel in each subordinate organization was never enough to meet the requirements, a solution that proved effective was to adopt the principles in a networked CDPS approach.⁴⁵

By adding the automated collaborative tools at every headquarters and capitalizing on Internet technologies, the organization was able to circumvent the hierarchical military structure and achieve a cooperative distributed analytic structure. This allowed the analytic teams assigned to the subordinate commands to be immediately responsive with tailored analytic products to support their command while simultaneously supporting the solution of the broader analytic problems of the higher and adjacent commands. Additionally, their analytic products benefited from the interaction with other analysts outside of the organization since it provided a broader context on which they could base their assumptions. Using the CDPS model, the tasks associated with the analysis of information in each of the subordinate commands was directly related to the broader problem set of the higher and adjacent commands. Each analytic node

remained apprised of the current assessment and participated in the future assessment by analyzing internally derived information and collaborating in near real time on the result. Thus, synergy was achieved by bringing together these distributed nodes of analytic capability. The Assistant Division Commander for Maneuver (ADCM) for the 4th Infantry Division dubbed this concept the Virtual Analytic Control Element or Virtual ACE concept.

VIRTUAL ANALYTIC CONTROL ELEMENT (ACE)

The Virtual ACE concept recognizes that the subordinate analytic elements of each headquarters in the architecture are producers of intelligence and are therefore nodal extensions of the larger intelligence community. The senior Intelligence Officer in the 4th Infantry Division, had no direct authority over subordinate intelligence elements within the hierarchy and therefore was limited to a supervisory responsibility for the process. It took command influence from the decisionmaker to implement the concept successfully. While this appears to be a centralized approach, a subtle differentiation exists. The authority for decisionmaking remained centralized, while the execution of the analytic process remained distributed and collaborative.

Each intelligence team was required to task its assets, process sensor data and collect reports from organic assets as they normally do. In addition to providing tailored intelligence products to their supported headquarters, they were required to share the results of their analysis with the rest of the networked community. Thus, each element produced a detailed assessment of its Area of Intelligence Responsibility (AOIR). The Internet and supporting software allowed a means to share the results of analysis in near-real-time (NRT) and not simply pass the data to be re-analyzed by the next higher Headquarters and visa versa. The ability to share analyzed information in NRT and to collaborate on the analysis with others allowed the entire network to compare the results of analysis and come to consensus on the assessment very rapidly. This collaborative approach kept the entire network apprised of the current assessment and provided a means to resolve discrepancies between echelons using the underlying data, if required. Of course, if any headquarters needed the underlying data, it was available on the network in distributed databases and could be automatically "pushed" or "pulled" by any analyst and used in making their assessments locally if required. Generally, however, the requirement for timely assessments of the enemy situation demanded that analysts collaborate on the situation as they saw it and not the supporting data. The supporting Internet technology allowed analysts to simply take the situation as seen by the subordinate

units and incorporate it into their assessments to form a consolidated assessment of the current situation in near real time. (See Figure 1)

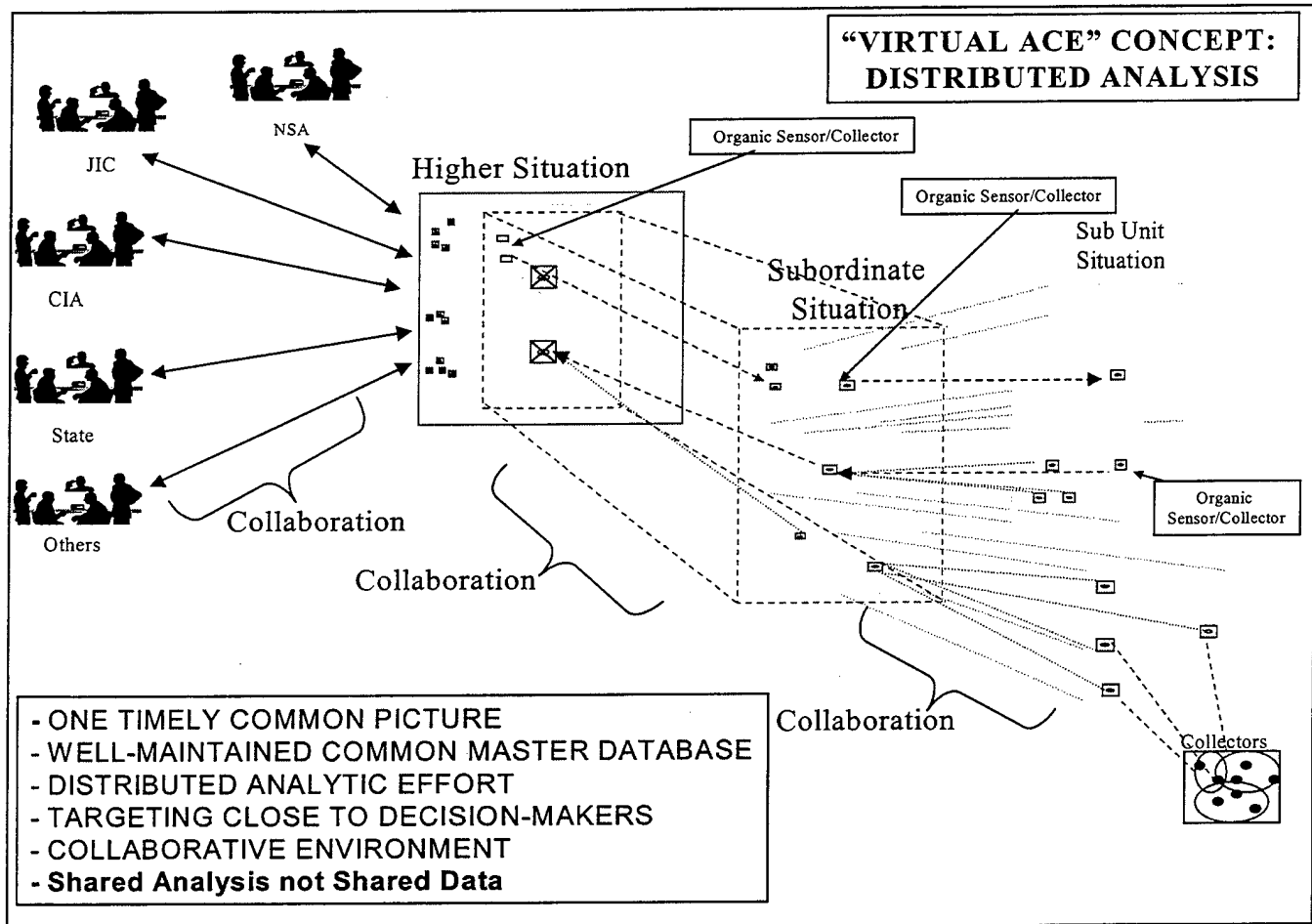


Figure 1 – THE “VIRTUAL ACE”

The virtual ACE concept formed all elements of the 4th Infantry Division’s intelligence community into a near real time collaborative working group that solved the larger problem of analyzing the current situation for the community while retaining the ability to satisfy the specific requirements of the supported command. It embraced the idea that those closest to the problem are probably the ones with the most insight into the issue. It also recognized that the alternative views of other analysts in the architecture were valuable in assessing the situation and defining alternative possibilities. The collaborative tools allowed everyone to achieve a broader understanding of the situation and allowed the entire organization to capitalize on the intellectual capabilities of the organization as a whole, not just those supporting a single echelon

of command. This process required a significant cultural change to motivate the personnel to conduct collaborative analysis and included two major challenges that took time and significant leadership to overcome. The first was an issue of trust and the second was the competition between analytic elements.

The organization's culture of distrust for subordinate analytic expertise was the result of experience, and the lack of modern technology. Previously, information that passed from higher-to-lower and visa versa was out of date. Analysts at each headquarters grew to lack faith in the analytic expertise of those that were reporting since each viewed their problems from a parochial perspective. When the organization changed its methods, analysts had to work in a collaborative manner. As a result, analysts, over time began to trust the information that they shared and the analytic capabilities of the individuals involved.

Even within the tactical force, each level of command wanted to demonstrate their competency by being the first to "make the call" on what was happening and what would happen. The virtual environment and collaborative approach to analysis allowed the analysts to share equally in the analytic task and the credit. Thus, the process allowed them to come closer to a consensus on what the assessment would be. Analysts usually worked out their differences of opinion by evaluating the details that led to the judgments. When analysts could not agree, the senior analyst would make a final decision on the assessment and disagreements identified as alternative views.

DISTRIBUTED COLLABORATIVE ANALYSIS – A NEW APPROACH FOR THE COMMUNITY

The National Intelligence Community finds itself in much the same situation as the tactical intelligence community found itself before the AWE, and in which Lockheed Martin found itself in the 1990s. It remains a hierarchical structure contending with an environment characterized by ambiguous and constantly changing threats. The rapid pace of growth in information technologies has caused decisionmakers at all echelons to demand that the community become more responsive and agile in meeting their demands for intelligence. As was noted in the National Performance Review of 1993, "the end of the Cold War and pressing domestic issues have created a strong mandate for changing the degree in which elements of the Intelligence Community must act as a team."⁴⁶

Some in the Intelligence Community are making good use of many of the virtual office tools, because of the existence and improvement in Intelink in its various forms. For the most

part, however, the community has chosen to concentrate on providing more products as opposed to developing an environment for rapid teaming and near real time collaboration.

There are also many good plans on the horizon. One example is the Community Intelligence Collection Management Program (CICMP), co-sponsored by CIA and DIA. Their goal is to provide a single architecture for the management of intelligence requirements. Once an analyst has an information requirement, he can query a master database of requirements to see if someone in the community has already answered the requirement or if another analyst has already requested it. If it is not in the system, he enters the information requirement, where it remains visible to all. A system such as this would significantly improve the efficiency of collection management processes throughout the community, and add to the collaborative environment, so long as tactical level analysts can interface and access it using tactical collection management systems based on a common set of standards.

Nonetheless, while efforts are being made across the Intelligence Community to address the need for collaborative analysis, they are not as pervasive as they could be. An excellent example to demonstrate this point is in the area of "national support to military operations." As a direct result of the expansion and diversity of threats, and the compression of the strategic and tactical levels of intelligence, theater and tactical intelligence officers have increasingly looked to the national Intelligence Community to fulfill their information and analytic shortfalls in support of deployed forces. The Intelligence Community developed the National Intelligence Support Team (NIST) to accommodate this need.⁴⁷

The NIST is a nationally sourced team made up of intelligence and communications experts from the Central Intelligence Agency, Defense Intelligence Agency, the National Security Agency, or other national agencies. Its purpose is to provide a tailored national level, all-source intelligence team to deploy, with a Joint Task Force (JTF) Commander, during crisis or contingency. Its major missions include coordination with its parent organizations, analytical expertise, I&W, special assessments, targeting support, access to National databases, and facilitating requests for information from national assets as well as analytic capability.⁴⁸

The Intelligence Community originally intended the NIST to allow increased access to national level support. They provided communications, and computer technology, that was unfamiliar to the supported analysts and incompatible with other communications in the command.⁴⁹ In addition to providing access, these individuals brought with them analytic expertise, and knowledge of the capabilities and limitations of their organizations.

Today, we have partially closed the gap in communications and computer technology in the theater and tactical force. The systems and communications that the NIST continues to

deploy are now organic to the organizations that they support. Since these systems are redundant, the primary role of the NIST has changed. The existence of the teams today, appears to serve more as a gateway to the supporting organizations than as a facilitator of communications. Given the current state of technology, a more open architecture could facilitate collaboration between the supported JTF and the supporting agency without the use of this "go-between." Eliminating the NIST, and putting those personnel back into the supported organizations, would significantly enhance their ability to meet the supported headquarters needs. It would also allow them to be the element that the JTF reaches back to, rather than deploying them forward. Thus, it assures that the resources would be available before and during deployment when the JTF needs them the most.

The lessons learned from the Bosnia missions seem to support this idea. For example, the requirement for six teams in Bosnia for a year duplicated intelligence efforts, reduced national agencies' capabilities to provide support to other potential crises, and depleted valuable, limited national intelligence resources, including personnel and sophisticated equipment.⁵⁰ Once again, opening the architecture to allow a collaborative environment between the supporting agency and supported command would free up these valuable resources and allow them to support the JTF without being physically co-located. The barriers to achieving this goal are improvements in collaborative tools, communications, access, and training.

The solution for the community is to adopt a more flexible, redundant approach to analysis. Much like Lockheed Martin in the 1990's, the Intelligence community must determine a means of organizing the intelligence expertise that exists throughout the world so that it may deliver intelligence products that meet the varying needs of the intelligence consumers with the speed of a smaller organization and reorganize just as quickly as the conditions and opportunities change.⁵¹ An approach is to adopt the CDPS model that distributes analysis among the analytic agencies and capitalizes on rapid teaming using collaborative tools, the Internet, and new software solutions such as the virtual office. As indicated previously, the collaborative and distributed approach to analysis will allow for the simultaneous solution of many smaller problems that are related to a larger analytic problem by making the most efficient use of the intellectual capital throughout the community. It also retains the unique perspectives of the analysts that result from the close association with the customers they support. Finally, it will achieve an enhanced ability to contend with the speed and complexity of the information age by allowing for the rapid development of communities of interest to work on specific issues without having to reorganize.

THE CHALLENGES TO ACHIEVING DISTRIBUTED COLLABORATIVE ANALYSIS

While new technologies offer tremendous potential, the mere existence of an efficient communications network does not guarantee that an organization will use it and perform as expected.⁵² To build a collaborative working environment between organizations requires quality people that are motivated to do so. Additionally, it requires a high quality operating system, resources, and a steering process. It also requires a culture of trust and joint problem solving, and leadership that manages a development process.⁵³

The Intelligence Community clearly has quality people that are highly capable in each of the intelligence disciplines, and the resources to meet most mission requirements appear to exist. There seems to be four critical elements that preclude the implementing this model today. The national Intelligence Community lacks a common standard for the implementation of the intelligence architecture, which adversely affects the ability to interoperate. It must deal with the issue of multi-level security. It must adopt a culture of trust and joint problem solving that is crucial for the implementation of a CDPS approach. Finally, the community must establish a means to overcome the issue of the competing priorities between internal and external analytic requirements.

The first challenge for the intelligence community is common standards for implementing the intelligence architecture. While Intelink provides a common backbone for access to intelligence products, the community continues to suffer a lack of hardware system interoperability that does not adhere to a common set of standards.⁵⁴ Even today, the community cannot seamlessly convert databases, share map data, or operate outside a web-based environment. A current example is the requirement to convert the Intelligence Database (IDB) into a form usable by the Army's All Source Analysis System (ASAS) All Source Correlated Database (ASCDB). The capability exists to accomplish the conversion, but it takes time and effort to do so. These types of problems are not isolated to the national Intelligence Community but are also prevalent among the military intelligence services. This incompatibility runs counter to any effort to achieve a collaborative approach to analysis. Crucial to success of the CDPS approach is the development of and adherence to a common communications standard integrated into a global information grid that is accessible by all intelligence organizations and analysts.

Probably the single most difficult challenge for achieving a truly distributed collaborative analytic environment is the issue of multi-level security. The distributed collaborative environment creates a contradiction. The issue boils down to balancing the risks associated

with an open information environment against protecting the information from unauthorized disclosure. This problem is not new. As far back as 1996, Emmett Paige, then Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, identified this issue in his comments to the Intelink Mission Support Conference in San Diego.⁵⁵ Today, the solution is to carve up the Intelink network into separate levels of security based on levels of access. For example, Intelink – U is for unclassified information, and Intelink-SCI is for compartmented information. The crafters of these networks have physically separated them so that analysts cannot gain access without the proper hardware and cryptographic tools. Given today's technology, new tools must be developed that allow an analyst to be called or paged across these networks and move to collaborative work areas where analysts can gather to evaluate a common issue in a work environment at the appropriate security level.

The Intelligence Community further complicates the security issue by its propensity to over-classify information. This runs counter to the information revolution and efficiency.⁵⁶ Compartmentalization and classification are impediments to the free flow of information that are inherent in the virtual organizations and teams within the business community. System developers must build mechanisms into the architecture that facilitate the free flow of information rather than impeding it. "Powerful concepts demand a guiding vision of equal power."⁵⁷ Like Intelink, the concept of distributed collaborative analysis "will realize its promise if we do not lose sight of what it is supposed to do for us and learn to use it to our best advantage."⁵⁸

Another obstacle to achieving this team approach is cultural.⁵⁹ In order to adopt this new method for analysis it is crucial to form an environment of trust and joint problem solving. To do so will require the elimination of the culture of competition and the adoption of a team culture that permeates the entire community.

The culture of competition within the Intelligence Community was not by design. Instead, it resulted from its hierarchical structure and differing missions. For example, the Central Intelligence Agency is focused on supporting the President and his National Security Council, other policy makers secondarily and the remainder of the national intelligence community in a tertiary manner. The departmental intelligence agencies are focused primarily on supporting their departmental masters and anyone else as a secondary effort.⁶⁰

During the Cold War, the Defense Intelligence Agency consistently supported the "worst case" interpretations of data in order not to undercut the Secretary of Defense's and the Chairman's budgets and perhaps risk the nations warfighting capability. The Central Intelligence Agency, on the other hand, had a different focus. Therefore, it made its

interpretations based on other factors. The State Department's Bureau of Intelligence and Research frequently based its judgments on how the intelligence would support the Secretary of State's policy. Finally, the military service intelligence organizations were always mindful of their respective service budgets for much the same reasons as the Defense Intelligence Agency. For example, during the Cold War, no reduction of the estimate of the Soviet naval threat was going to find support from US Naval Intelligence.⁶¹

This competitive culture was reinforced in 1976 when President Ford created a special team of outside experts known as the "B" Team to challenge the National Intelligence Estimate. Thus, the competition for resources in the Intelligence Community has led to an environment of distrust between agencies and organizations.⁶² As a result, many individuals in the community do not consider their job to include the larger role of being part of the overall intelligence team. Rather, they see themselves as members of a select intelligence element whose purpose is to support their decisionmaker and must compete for resources in order to do so. The Intelligence professional of the future must have the ability to move in and out of different alliances of colleagues depending on the issue.

Finally, in a resource-constrained environment, there are concerns that implementing this approach would impinge on the priorities of the organizations involved and devolve into an informal means of tasking. With their differing missions and the competition for resources, none within the community are going to be willing to adopt a system that allows them to be tasked by external organizations and agencies at the same level of priority as their internal tasking mechanism.⁶³

The parties involved must not view the collaborative approach as a means of tasking or a burden to the organization. Participation in a collaborative environment must serve a purpose. Either the organization must benefit by being a member of the community of interest, or it must serve a higher purpose based on national priorities or a specific crisis. Regardless, the Intelligence Community will need to develop policy and procedures for implementing this approach that does not intrude on the specific missions of the organizations involved.

Ultimately, adopting the Distributed Collaborative Analysis approach may facilitate a shift in view over time. As agencies are forced to work collaboratively and in a distributed manner, the momentum associated with success may further motivate individuals to want to participate.

CONCLUSION

In this post-Cold War environment, the threats to the U.S. National Security have grown more complex, dynamic, and uncertain.⁶⁴ These trends significantly challenge the Intelligence

Community to deal with a broader spectrum of potential threats than during the Cold War period. Additionally, the rapid growth in information age technologies has significantly compressed the dimensions of time and space.

As a result, the intelligence requirements are in a constant state of flux, reflecting changing policymaker needs and the evolving world situation. These strategic trends demand an Intelligence Community that can dominate the full spectrum of economic, political and military intelligence by becoming more responsive and agile in meeting consumer demands for intelligence. The Intelligence Community must maintain sufficient flexibility to respond rapidly and efficiently to the changing intelligence environment. It must accommodate significant international changes in political alliances, military threats, and opportunities of all sorts; technological change affects the world economic, political, and military balances as well as the abilities of technical intelligence collection systems. We cannot define the organizational structure and specific roles in a static, hierarchical way that too narrowly focuses responsibilities. We must remain more flexible than ever before. In the 1980s, the CIA began creating pools of analysts and collectors to handle terrorism, counterterrorism, narcotics, and weapons proliferation issues. The CIA regularly reallocates resources to changing priorities and restructures to meet the requirement. In a networked environment, the costs associated with flexibility can be significantly reduced and allow for more rapid responses to changing situations.

While the cultural shifts needed to implement a CDPS approach appear daunting, the best solution for the Intelligence Community appears to be to divest itself of the Cold War analog methods characterized by stovepiped, hierarchical approaches to analysis. In order to remain relevant in the information age, it must embrace a new method for analysis. An approach based on Cooperative Distributed Problem Solving, the use of Internet technologies, and the virtual organization. Doing so will significantly enhance the community's ability to capitalize on the analytic capabilities of the nation while mitigating the effects of the expanding diversity of threats, the growth of information technologies, the lack of governmental support for intelligence at any cost⁶⁵ and the compression of time and space.

WORD COUNT = 10,571

ENDNOTES

¹ William J. Clinton, A National Security Strategy for a New Century (Washington D.C.: The White House, October 1998), p 2-3

² John December, "Transitions in Studying Computer- mediated Communication," Computer Mediated Communication Magazine, Volume 2, Number 1, 1January 1995; available from <<http://www.december.com/cmc/mag/1995/jan>>; Internet; accessed 21 Jan 2001.

³ Jeffrey T. Richelson, A Century of Spies: Intelligence in the Twentieth Century (New York: Oxford University Press, 1995), p 2

⁴ Michael H. Brackett, "Business Intelligence Value Chain," 21 Jan 2001; available from <http://www.dmreview.com/portal_ros.cfm?NavID=91&EdID=115&PortalID=17>; Internet; accessed 21 Jan 2001.

⁵ Abram N. Shulsky, Silent Warfare: Understanding the World of Intelligence, 2nd Ed., rev. by Gary J. Schmitt (New York: Brassey's, 1993), p 45

⁶ Ibid.

⁷ Department of Defense, National Intelligence Support to Joint Operations, Joint Publication 2-02 (Washington, D.C.: U.S. Department of Defense, 28 Sept 1998), p GL-6

⁸ Jeffrey T. Richelson, The U.S. Intelligence Community, 4th Ed., (Boulder, Colorado: Westview Press, 1999), p 3

⁹ John P. Finnegan, The Military Intelligence Story: A Photographic History, (Fort Belvoir, Va.: History Office of the Chief of Staff, USINSCOM, 1994), p 1

¹⁰ Richelson, A Century of Spies: Intelligence in the Twentieth Century, p 3-4

¹¹ Finnegan, p 2

¹² Richelson, A Century of Spies: Intelligence in the Twentieth Century, p 3-4

¹³ Ibid p 7

¹⁴ Ibid p 7

¹⁵ Finnegan p 3

¹⁶ Finnegan p 11

¹⁷ Shulsky p 22-23

¹⁸ Finnegan, John P., The Military Intelligence Story: A Photographic History (Fort Belvoir, Va.: History Office of the Chief of Staff, USINSCOM, 1994), p 11

¹⁹ Mark M. Lowenthal, Intelligence: From Secrets to Policy (Washington, D.C.: CQ Press, 2000), p 11

²⁰ Richelson, A Century of Spies: Intelligence in the Twentieth Century, p 131

²¹ Richelson, A Century of Spies: Intelligence in the Twentieth Century, p 131-133

²² Lowenthal, p 12

²³ Richelson, The U.S. Intelligence Community, p 17-18

²⁴ Richelson, The U.S. Intelligence Community, p 13

²⁵ Lowenthal, p 13

²⁶ Ibid

²⁷ Ibid

²⁸ Ibid

²⁹ Bruce D Berkowitz and Allan E. Goodman, Best Truth: Intelligence in the Information Age (New Haven, Conn.: Yale University Press, 2000) p ??

³⁰ John C. Gannon, "The CIA in the New World Order: Intelligence Challenges through 2015," 1 February 2000; available from <http://www.cia.gov/cia/public_affairs/speeches/dci_speech_020200smithson.html>; Internet; accessed 3 December 2000.

³¹ John E. McLaughlin, "New Challenges and Priorities for Analysis," Defense Intelligence Journal, Fall 1997; available from <<http://www.cia.gov/cia/di/speeches/428149298.html>>; Internet; accessed 3 December 2000.

³² Sean Gregory, "Economic Intelligence in the Post Cold War Era Issues for Reform," February 10, 1997; available from <<http://www.fas.org/irp/eprint/snyder/economic.htm>>; Internet; accessed 3 December 2000.

³³ Central Intelligence Agency, A Consumer's Guide to Intelligence (Washington, D.C: Office of Public Affairs) p 17

³⁴ Gannon

³⁵ "The Intelligence Community: National Performance Review," Sept 1993 (Washington D.C.: Office of the Vice President) pg 5

³⁶ Melissa A. Patrick, Intelligence in Support of Peace Operations: The Story of Task Force Eagle and Operation Joint Endeavor, Strategy Research Project (Carlisle Barracks: U.S. Army War College, Date April 2001), p 20-16

³⁷ Central Intelligence Agency, "Intelligence Analysis in the DI: Frequently asked Questions," available from <<http://www.odci.gov/cia/di/work/analyst.html>>; Internet; accessed 12 December 2000.

³⁸ "Cooperative Distributed Problem Solving," available from <<http://dis.cs.umass.edu/research/cdps.html>>; Internet; accessed 12 December 2000.

³⁹ "Cooperative Distributed Problem Solving." available from <http://centaurus.cs.umass.edu/~decker/latex/coord/section3_2.html>; Internet; accessed 12 December 2000.

⁴⁰ "Cooperative Distributed Problem Solving," available from <<http://dis.cs.umass.edu/research/cdps.html>>; Internet; accessed 12 December 2000.

⁴¹ Robert Moskowitz, "Variations On Alternative Officing Strategies Now Taking Hold," 1998; available from <<http://www.yoyow.com/rmoskowitz/alt-office.html>>; Internet; accessed 5 November 2000.

⁴² Eric K. Shinseki, "The Army Transformation: A Historic Opportunity", Army Magazine (October 2000) p 21-30

⁴³ Michael W. Powell, "MI Systems Transformation." Military Intelligence, (Unpublished Article, Military Intelligence Center and School, Ft Huachuca Az., 2001)

⁴⁴ Robert W. Jr. Noonan, "Military Intelligence: Force Multiplier In Army Transformation." Army Magazine, October 2000, p 137-140.

⁴⁵ The ideas in this paragraph are based on personal experience of the author as Commander of the 104th MI Battalion during the Division Advanced Warfighting Experiment (DAWE) 1997.

⁴⁶ "The Intelligence Community: Accompanying report of the National Performance Review," p 5

⁴⁷ James M. Lose, "National Intelligence Support Team," Studies in Intelligence (Winter 1999-2000) (Unclassified Edition): p 94.

⁴⁸ Joint Chiefs of Staff, National Intelligence Support to Joint Operations, Joint Pub 2-02, (Washington, D.C.: GPO, November 1997), pV5-6.

⁴⁹ James M. Lose, "National Intelligence Support Team," Studies in Intelligence (Winter 1999-2000) (Unclassified Edition): p 94.

⁵⁰ Lt. Cdr. Paul Jeager, USN, Operation Joint Endeavor, Joint Universal Lessons Learned, Draft 30 Jan. 1997, p 2

⁵¹ Berkowitz, p 75

⁵² Eugene Bardach, Getting Agencies to Work Together: The Practice and Theory of Managerial Craftmanship (Washington, D.C.: Brookings Institution Press, 1998) p 27

⁵³ Ibid p 310

⁵⁴ "The Intelligence Community: Accompanying report of the National Performance Review," p 17

⁵⁵ Emmett Paige, "The Rapid Expansion of Intelink," prepared remarks to the Intelink Mission Support Conference, San Diego, June 11, 1996. Available from <<http://www.fas.org/irp/program/disseminate/intelink.htm>>; Internet; accessed 18 Mar 20

⁵⁶ Berkowitz, p 151

⁵⁷ Paige

⁵⁸ Ibid

⁵⁹ Ibid

⁶⁰ Anthony R. Williams, DCI Representative to the U.S. Army War College; interview by author, 2 April 2001, Carlisle Barracks, PA.

⁶¹ Williams

⁶² Codevilla, p 208-209

⁶³ Williams

⁶⁴ Clinton, p 2-3

⁶⁵ Berkowitz, p 24

BIBLIOGRAPHY

Alberts, David S., John J. Garstka, and Frederick P. Stein. Network Centric Warfare: Developing and Leveraging Information Superiority. Washington, D.C.: DOD C4ISR Cooperative Research Program, 1999.

Assistant Director of Central Intelligence for Collection, "ADCI Accomplishments". Available <<http://www.cia.gov/cia/publications/fy98intellrpt/accomplish.html>>. Internet. Accessed 3 December 2000.

Bardach, Eugene. Getting Agencies to Work Together: The Practice and Theory of Managerial Craftsmanship. Washington, D.C.: Brookings Institution Press, 1998.

Baron, Talila. "OLAP goes online – Web Lets Companies Offer Analysis to More Employees." 20 September 2000. Available from <<http://www.informationweek.com/753/olap.htm>>. Internet. Accessed 5 December 2000.

Bergert, Stacy. "Power to the People: Getting the Right Information to the Right Decision Makers is a Complex Process, but Automating the Data Staging Process can help." December 2000. Available from <<http://www.intelligentkm.com/feature/06/feat1..shmtl>>. Internet. Accessed 5 December 2000.

Berkowitz, Bruce D. and Allan E. Goodman. Best Truth: intelligence in the information age. New Haven: Yale University Press, 2000.

Brackett, Michael H. "Business Intelligence Value Chain." 21 Jan 2001. Available from <http://www.dmreview.com/portal_ros.cfm?NavID=91&EdID=115&PortallID=17>. Internet. Accessed 21 Jan 2001.

Central Intelligence Agency. A Consumer's Guide to Intelligence. Washington, D.C.: Office of Public Affairs.

_____. "Intelligence Analysis in the DI: Frequently asked Questions." Available from <<http://www.odci.gov/cia/di/work/analyst.html>>. Internet. Accessed 12 Dec 2000.

_____. "Psychology of Intelligence Analysis 1999." Available from <<http://www.cia.gov/csi/books/19104/art7.html>>. Internet. Accessed 3 December 2000.

Clinton, William J. A National Security Strategy for a New Century. Washington D.C.: The White House, October 1998.

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

"Cooperative Distributed Problem Solving." Available from <http://centaurus.cs.umass.edu/~decker/latex/coord/section3_2.html>. Internet. Accessed 12 December 2000.

"Cooperative Distributed Problem Solving". Available from <<http://dis.cs.umass.edu/research/cdps.html>>. Internet. Accessed 12 December 2000.

Council on Foreign Relations. "Making Intelligence Smarter: The Future of U.S. Intelligence." 1996. Available from <www.fas.org/irp/cfr.html>. Internet. Accessed 13 Nov 2000.

Cunningham, Kevin R. Bounded Rationality and Complex Process Coupling: Challenges for the Intelligence Support to Information Warfare. Strategy Research Project. Carlisle Barracks: U.S. Army War College, April 2000.

Davis, Jack. "The Challenge of Managing Uncertainty: Paul Wolfowitz on Intelligence Policy – Relations." Available from <<http://www.cia.gov/csi/studies/96unclass/davis.htm>>. Internet. Accessed 3 December 2000.

December, John. "Transitions in Studying Computer-Mediated Communication." 1 Jan 1995. Available from <http://www.december.com/cmc/mag/1995/jan/december.html>. Internet. Accessed 5 December 2000.

Department of Defense. National Intelligence Support to Joint Operations, Joint Pub 2-02. Washington D.C.: Department of Defense, 28 Sept 1998.

John P. Finnegan. The Military Intelligence Story: A Photographic History. Fort Belvoir, Va.: History Office of the Chief of Staff, USINSCOM, 1994.

Friedman, George and Meredith. Future of War: Power, Technology and American World Dominance in the Twenty-First Century. New York: St Martins Press, 1998.

Friedman, Mark H. "Barrier Bashing: Successful knowledge management initiatives rely heavily on a balance between people and technology." Available from <http://www.intelligentkm.com/feature/06/feat1.shtml>. Internet. Accessed 5 November 2000.

Gannon, John C. "Managing Information in the Directorate of Intelligence." 27 March 1997. Available from <http://www.cia.gov/cia/di/speeches/42884797.html>. Internet. Accessed 3 December 2000.

_____, John C. "The CIA in the New World Order: Intelligence Challenges through 2015." 1 February 2000. http://www.cia.gov/cia/public_affairs/speeches/dci_speech_020200smithson.html. Internet. Accessed 3 December 2000.

Gentry, John A. "A Framework for Reform of the U.S. Intelligence Community." 6 June 1995. Available from <http://www.fas.org/irp/gentry>. Internet. Accessed 13 Nov 2000.

Gregory, Sean. "Economic Intelligence in the Post Cold War Era Issues for Reform", Available from <<http://www.fas.org/irp/eprint/snyder/economic.htm>>. Internet. Accessed 3 Dec 2000.

Hedley, John Hollister. "Checklist for the Future of Intelligence." March 1995. Available from <<http://sfswww.georgetown.edu/sfs/programs/isd/files/intell.htm>>. Internet. Accessed 5 December 2000.

_____, John Hollister. "The Intelligence Community: Is it broken? How to fix it?" Available from <<http://www.cia.gov/csi/studies/96unclass/hedley.htm>>. Internet. Accessed 3 December 2000.

Holt, Pat M. "Our Culture of (Over) Secrecy." 7 December 2000. Available from <<http://ebird.dtic.mil/Dec2000/e20001207our.htm>>. Internet. Accessed 7 December 2000.

Lose, James M. "National Intelligence Support Team." Studies in Intelligence Winter 1999-2000 (Unclassified Edition).

Lowenthal, Mark M. Intelligence: From Secrets to Policy. Washington, D.C.: CQ Press, 2000.

McLaughlin, John E. "New Challenges and Priorities for Analysis." Fall 1997. Available from <<http://www.cia.gov/cia/di/speeches/428149298.html>>. Internet. Accessed 3 December 2000.

Mitre Corporation. "Collaborative Virtual Workspace." 13 October 2000. Available From <<http://cvw.sourceforge.net/cvw/info/CVWOverview.php3>>. Internet. Accessed 5 November 2000.

Moskowitz, Robert. "Variations On Alternative Officing Strategies Now Taking Hold." 1998. Available from <<http://www.yoyow.com/rmoskowitz/alt-office.html>>. Internet. Accessed 5 November 2000.

Noonan, Robert W. Jr. "Military Intelligence: Force Multiplier In Army Transformation." Army Magazine, October 2000.

"Improving Intelligence Analysis". Available from www.fas.org/irp/offdocs/int012.html. Internet. Accessed 13 November 2000.

Jeager, Lt. Cdr. Paul. USN. Operation Joint Endeavor, Joint Universal Lessons Learned, Draft 30, Jan. 1997

Paige, Emmett. "The Rapid Expansion of Intelink." Prepared remarks to the Intelink Mission Support Conference, San Diego, June 11, 1996. Available from <http://www.fas.org/irp/program/disseminate/intelink.htm>. Internet. Accessed 18 Mar 2001.

Patrick, Melissa A. Intelligence in Support of Peace Operations: The Story of Task Force Eagle and Operation Joint Endeavor. Strategy Research Project. Carlisle Barracks: U.S. Army War College, April 2000.

Powell, Michael W. "MI Systems Transformation." Unpublished article. Military Intelligence Center and School, Ft Huachuca, Az., 2001

Quirk, Richard J., III. "Training the MI Force for the Future." Unpublished article. Military Intelligence Center and School, Ft Huachuca, Az., 2001

Richelson, Jeffrey T. A Century of Spies: Intelligence in the Twentieth Century. New York: Oxford University Press, 1995.

_____, Jeffrey T. The U.S. Intelligence Community. 4th ed. Boulder, Colorado: Westview Press, 1999.

Shinseki, Eric K. "The Army Transformation: A Historic Opportunity." Army Magazine, October 2000. p 21-30

Shulsky, Abram N. Silent Warfare: Understanding the World of Intelligence. 2nd ed. rev. by Gary J. Schmitt. New York: Brassey's, 1993.

Tenet, John J. "The Worldwide Threat in 2000: Global Realities of Our National Security." 2 February 2000. Available from http://www.cia.gov/cia/public_affairs/speeches/dci_speech_020200.html. Internet. Accessed 3 December 2000.

"The Intelligence Community, National Performance Review." Sept 1993. Washington D.C.: Office of the Vice President.

Thomas, John D., Jr. "MI Is Out Front in Army Transformation." Unpublished article. Military Intelligence Center and School, Ft Huachuca, Az., 2001

Travers, Russ. "The Coming Intelligence Failure." Available from <http://www.odci.gov/csi/studies/97unclass/failure.html>. Internet. Accessed 6 December 2000.

Williams, Anthony R., DCI Representative to the U.S. Army War College. Interview by author, 2 April 2001, Carlisle Barracks, PA.