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.

INFORMATION MANAGEMENT IN THE JTF

BY

LIEUTENANT COLONEL JENNIFER NAPPER
United States Army

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

USAWC CLASS OF 2002

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

20020806 324

USAWC STRATEGY RESEARCH PROJECT

INFORMATION MANAGEMENT IN THE JTF

by

Lieutenant Colonel Jennifer Napper
United States Army

COLONEL Ralph Ghent
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: Jennifer Napper

TITLE: Information Management in the JTF

FORMAT: Strategy Research Project

DATE: 09 April 2002 PAGES: 34 CLASSIFICATION: Unclassified

Commanders are drowning in information as staffs try to meet their information needs. Subordinate and higher headquarters flood the telecommunications networks with data to ensure everyone gets all the latest updates. The joint vision for the future is based upon network centric warfare enabled by information superiority. Most of the Department of Defense efforts are focused on the networks required to support future operations. But who decides what information is needed? This paper looks at current operations and the vision for the future to discern how the Information Manager will ensure the right information gets to the commander at the right place and time.

TABLE OF CONTENTS

ABSTRACT III

LIST OF ILLUSTRATIONS VII

LIST OF TABLES IX

INFORMATION MANAGEMENT IN THE JTF 1

- "THE RIGHT INFORMATION" 2
- "THE RIGHT PLACE AT THE RIGHT TIME" 3
- OPERATION JOINT FORGE: A CASE STUDY IN INFORMATION MANAGEMENT 4
- COMMAND AND CONTROL 4
- NATO Communications 5
- Coalition Communications 6
- U.S. Communications 7
- REPORTING 8
- INFORMATION FLOW SUMMARY 8
- SOLUTIONS 8
- LESSONS FROM OPERATION JOINT FORGE 10
- JOINT VISION 2020: NETWORK CENTRIC WARFARE 11
- THE GLOBAL INFORMATION GRID 12
- INFORMATION DISSEMINATION MANAGEMENT 17
- SITUATIONAL UNDERSTANDING FROM DATA CHAOS 18
- CONCLUSIONS 20

ENDNOTES 21

BIBLIOGRAPHY 23

LIST OF ILLUSTRATIONS

FIGURE 1: C2 IN MND(N) 5

FIGURE 2: MULTIPLE LEVELS OF SECURITY IN OJF 6

FIGURE 3: MERCURY NETWORK 7

FIGURE 4: NETWORK CENTRIC WARFARE 11

FIGURE 5. THE GIG 13

FIGURE 6: CURRENT C4 APPLICATIONS 14

FIGURE 7: FUTURE C4 APPLICATIONS 15

LIST OF TABLES

TABLE 1. FUNCTIONAL CAPABILITIES OF IDM 18

INFORMATION MANAGEMENT IN THE JTF

The world geopolitical situation changed dramatically over the last decade. The breakup of the Soviet Union resulted in numerous new states, several other countries have had major changes in political structure, and many other states are failing. New threats toward the United States or its interests have emerged such as newly declared nuclear capable nations, or the transnational radical terrorists groups. The news channels and periodicals are overflowing with articles discussing the "new" or "asymmetric" threats.

To meet these new threats while harnessing many of the emerging technologies, the United States military is undertaking a sweeping revolution in military affairs. The transformation envisioned by General Hugh Shelton, Chairman, Joint Chiefs of Staff in Joint Vision 2020 includes a radical change in the way warfighters prosecute war and how they think about the enemy. This network centric warfare consists of a robustly networked force connecting everything from the sensors all the way to the shooters. The exponentially increased information sharing greatly enhances the quality of the information and permits a shared situational awareness, or joint common operational picture (COP). The COP facilitates collaboration and enhances the sustainability and speed of command. This synchronization and its synergistic effect will increase the military's ability to dominate operations across the full spectrum of operations by providing a clear detailed picture of the battlespace, dominant maneuver, self-synchronization of units, and increased precision engagement.[1]

Information superiority is not a new concept in warfighting. Commanders have always sought to have the advantage of seeing the enemy before the enemy saw them, of getting inside the enemy's decision cycle to more effectively change the outcome of a battle. War games and training center trends show that when forces see the enemy first, they usually win the battle decisively with few casualties. While the concept is not new, the digital revolution has dramatically changed the technology and processing that facilitate the commander's decision making abilities. Major General Scales notes that "...the increasing flow of information is quite literally drowning commanders, staffs, and intelligence organizations. This information overload challenge is one of the crucial by-products of the information age - one that we have yet to solve."[2] More than ever, getting the right information to the right place at the right time is critical to timely decisions.

This paper examines the information superiority vision espoused in Joint Vision 2020 and evolving support doctrine in Joint Publication 6-0, Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations; focusing on how

the J6 functions as the information manager facilitating the information dissemination in a Combined or Joint Task Force (JTF) in the future. It discusses current challenges for information managers as seen in the combined task force in Operation Joint Endeavor in Bosnia Herzegovina. Finally, it will propose a concept of how the J6 of a JTF might better ensure the information requirements of the commander and staff are met and the vision of information superiority translated into operational reality.

"THE RIGHT INFORMATION"

It is a generally accepted principle that command is both an art and a science. The art part is based on the commander's experience and some would say, his intuitive gift or gut instinct. Volumes are written on the military geniuses through the millennia. The science part of command is developed through years of education and is heavily dependent upon key information requirements. Commanders need certain elements of information before they are able or willing to make decisions. There have been numerous studies on precisely what information a commander needs before he can make those decisions. Five major studies commissioned by the Army from 1967 to 1986 all tried to reduce the scientific information requirements into a set of defined data that all commanders need.[3] One very detailed report developed a matrix of 38 essential information requirements for a corps commander, developed reports and standard operating procedures for presenting the data, and identified what communications means were available for disseminating the information.[4]

These ambitious studies fell short of realizing the full information requirements by assuming all commanders need the same information in all missions in order to make decisions. While there are some data required regardless of the commander or operation, for example maps and weather, radically different types of information might be required across the full spectrum of operations. Similarly, people process information differently: some visually, some verbally and some a combination of both. Therefore, information, even if complete, may need to be presented in a different format in order for the commander to process it. For example, statistical data can be presented in text format but may be easier for some to understand if shown in a bar graph.

As a commander processes information he builds a mental image from which he makes his decisions. He uses his current view of the situation; his own training, experience and understanding of doctrine; mission information from higher headquarters; and his intent to define and continually refine this mental model of the situation. Understanding how each commander builds his mental image of the enemy or friendly forces is critical to meeting his

information needs and facilitates "decision superiority – better decisions arrived at and implemented better than an opponent can react...."[5] If the information does not contribute to the overall understanding of the situation, it will be discounted or unused by the commander in making necessary decisions. "Information superiority provides the Joint force a competitive advantage only when it is effectively translated into superior knowledge and decisions."[6] Therefore, any successful attempt to define the commander's information needs must include both the right information in a usable format and an understanding of how the commander builds his image of the situation to make decisions.

"THE RIGHT PLACE AT THE RIGHT TIME"

"The JFC and subordinate commanders require the capability to obtain information from any location, at any time, and for any mission."[7] The second critical part of the equation is getting the information to the commander, wherever he may be, in time for him to make the decision. This portion of the equation focuses on the telecommunications systems and the management of the data flowing over the system. The J6 of a joint task force is clearly responsible for the planning, employing, and managing command, control, communications, and computer (C4) systems in support of joint operations. The J6 analyzes the mission, JFC's intent, situation and type of information systems required to provide decision support in order to develop a coherent, robust C4 infrastructure. "The C4 structure identifies elements that need to exchange information and consequently, C4 system terminations."[8] In other words, who needs to exchange information with whom? And what types of information?

Information is typically divided into "push" and "pull" categories. Push data includes both the routine, periodic universally required data and emergency, survival data. Updates to specific data within applications such as weather map updates or friendly location changes on a map all fall in the routine category. Early warning for air or missile threat certainly is emergency or survival data. Most of the efforts in situational awareness focus on "push" data.

"Pull" data is either unique or not as time sensitive. Types of data in this category include that found by going to an established web page for routine data or executing a query to find specific information from that web site. The difficulty arises in searching for information from other sites. Most search engines use special programs called "web crawlers" to examine pages and extract information that can be used to describe the pages. They store this data along with the internet web address for future use. These searches work best on text documents and can search for specific words or phrases.

There are two problems with using this form of retrieval: with stove-pipe systems the searches are limited to the interoperable applications and there are no standards for specific words or phrases. It might take a specific analyst hours to find the information before analysis can begin. Over the past five years there has been a substantial amount of work done to improve the automated classifying methods. One technique that holds a lot of promise for the military is the use of metadata tags. The intelligence community is making great strides in this particular area. They have developed the Intelligence Community Markup Language (ICML) to communicate information about the content of the document. It can even distribute information in accordance with different security classifications.

This process of getting the right information to the commander at the right place and time is extremely complicated and becomes even more difficult under transformation to the joint vision. Even a relatively simple operation such as the ongoing peacekeeping mission in Bosnia-Herzegovina is not easy. The following discussion on the mission from the G6 perspective shows the information dissemination challenges in a small coalition.

OPERATION JOINT FORGE: A CASE STUDY IN INFORMATION MANAGEMENT

The Stabilization Force in Bosnia-Herzegovina is a NATO peacekeeping mission divided into three areas of responsibility: multinational divisions north, southeast, and southwest. In October 2000 during the fifth year of the operation, 3rd Infantry Division (Mechanized) assumed responsibility for the Multinational Division North [MND(N)] region of Bosnia-Herzegovina. The C4I structure in Operation Joint Forge (OJF) is an excellent example of how complicated information management can be in a coalition force. To begin analyzing the C4ISR requirements and structure, the command structure and mission must first be understood.

COMMAND AND CONTROL

The mission of the division was to ensure a safe and secure environment for the implementation of the articles of the General Framework Agreement for Peace (GFAP) in Bosnia and Herzegovina. MND(N) consisted of five sectors: two U.S. battalions, the Nordic-Polish Battle Group (NORDPOL BG), the Turkish Battalion (TK BN), and the 1st Peacekeeping Russian Separate Airborne Brigade (PRSAB). As Figure 1 illustrates, the Battalions from the United States Army were assigned to MND(N), the NORDPOL BG and TK BN were under NATO operational control (OPCON) and the 1st PRSAB was supporting the mission but still assigned and controlled by the Russian Minister of Defense.

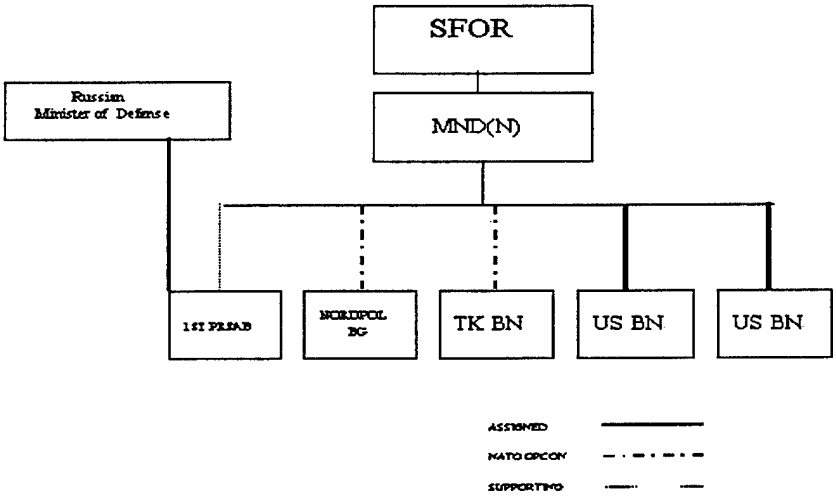

FIGURE 1: C2 IN MND(N)

This complicated C2 structure worked, but not without challenges. For example, since the PRSAB was not under any official command or control of the division, normal operational orders were not issued. Instead, instructions on implementing an operation were distributed explaining what was to be done and how it could be executed. Similarly, any changes to reporting requirements or communications were carefully worked at the chief of staff or command level prior to implementation. Further complicating command and control, each nation supporting the mission rotated their personnel on different time lines. The PRSAB had a yearly rotation but subordinate units staggered their rotations. The Turkish Battalion rotated as a complete unit every six months. The nearly constant turn-over of personnel necessitated simple orders and streamlined reporting procedures.

NATO Communications

The multinational environment required three different security classification systems. Overall SFOR was a NATO mission and therefore communications between SFOR Headquarters and its three divisions were conducted over NATO communications systems

named CRONOS. NATO security procedures were strictly enforced and NATO assigned personnel operated and maintained the network. These networks could interface with U.S. systems only for voice and did not interface with the coalition networks for voice or data.

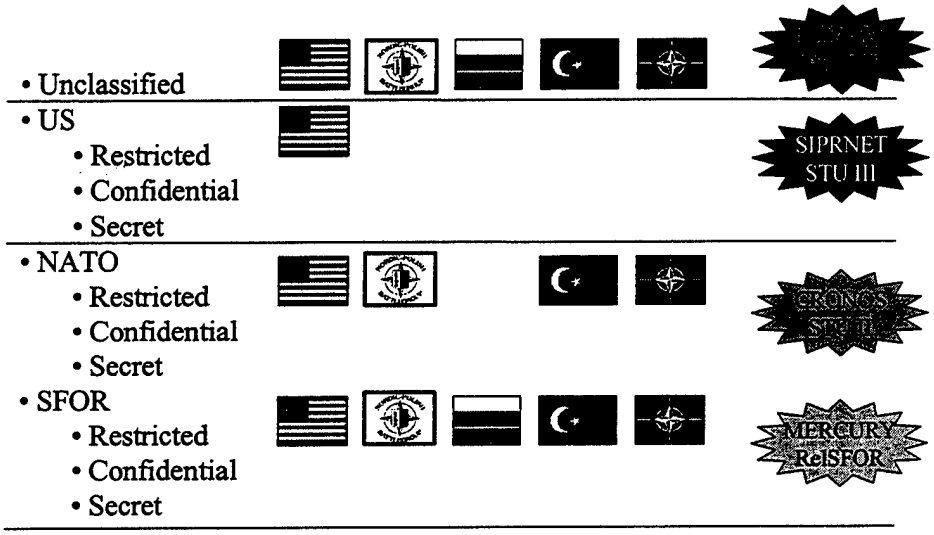

FIGURE 2: MULTIPLE LEVELS OF SECURITY IN OJF

There were two main data applications run on the NATO network: the Air Tasking Orders and Joint Operations/Intelligence Information System (JOISS). JOISS was utilized as a situation monitoring and assessment tool. Essentially, it is a database (utilizing Access), with a user-friendly front end for accessing and filtering human intelligence (HUMINT) information in the database. Unfortunately there was no clearly defined standard terminology for the data entered and some rotations did not enter any data at all. This led to difficulties searching the database and no confidence that the information was accurate or complete.

Coalition Communications

However, the coalition included non-NATO participants and therefore a separate network, run at the SECRET (releasable to SFOR) level was also utilized. This network (named MERCURY) connected the MND(N) Headquarters with all five subordinate units and provided both voice and data capability.

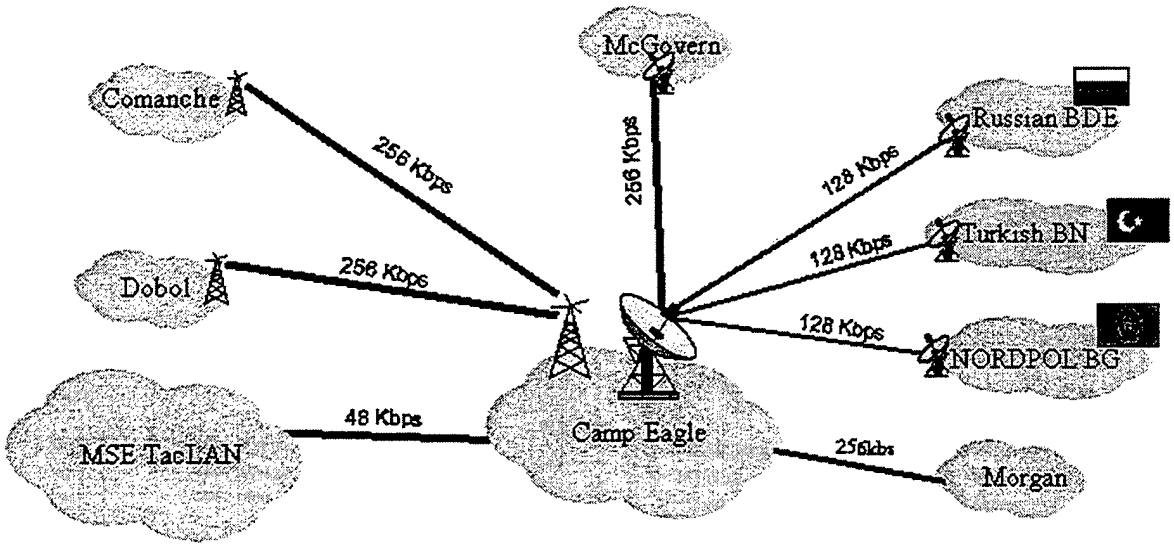

FIGURE 3: MERCURY NETWORK

The secure coalition network, including both the mail and web server, was owned and managed by the MND(N) personnel. Staff sections posted information to their own web pages and updated as needed. Since it was originally a very limited network, the first significant improvement in command and control for the MND(N) was extending the MERCURY net to all the staff sections in the division headquarters and increasing the number of users at each subordinate headquarters. In October 2000, the only database accessible on MERCURY was the weapon storage site (WSS) managed by the Joint Military Commission (JMC). Unfortunately, the data about recent inspections was not updated and the JMC had to double check the entire database.

U.S. Communications

The primary voice communications network (nonsecure and secure) was provided by a commercial vendor and extended to SFOR headquarters and all subordinate commands. A

commercial vendor managed the U.S. unclassified network and its interface into the NIPRNET. The U.S. classified networks were remotely managed from Heidelberg, Germany. This arrangement of separate, geographically dispersed network managers, though functional, complicated communications in Bosnia since managers were not always available to resolve issues as they arose. Several of the global applications were run on U.S. classified networks including the intelligence, weather, and Global Command and Control System (GCCS). Some information on the U.S. network (e.g. weather) was required by all personnel including the coalition partners. In these cases, manual interfaces (e.g. floppy disk transfer of data) were required.

REPORTING

At the beginning of SFOR 8, subordinate units submitted reports to the division by typing word documents and attaching them to an email. Staff sections would then consolidate the reports and fill in Power Point charts for the nightly update briefings. If the email was non-operational, units would use facsimile machines. While this method of reporting was functional, it was manpower intensive and data was lost. Staff sections were managing several databases, but they were not shared and accuracy of the data was questionable.

INFORMATION FLOW SUMMARY

Given the stove-piped applications and security segregation of all the information in MND(N), there was little situational awareness and even less information sharing. Subordinate units depended upon access to the Power Point slides briefed at the daily battle update brief to stay informed. Reporting was manpower intensive, cumbersome, and the coalition partners did not receive information in a timely manner. There was no emphasis on the use of databases, or information sharing. The best maintained records were in the G2, intelligence section, and these were classified for U.S. use only. Subordinate units understood their own sectors but knew very little, if anything, about adjacent sectors or situations in them that might affect their operations.

SOLUTIONS

In an attempt to improve reporting and information sharing, SFOR 8 initiated a new command and control reporting system. A web-based, database driven tool, TACWEB, provided operational information and situational awareness to all units and staffs within a common operating environment. Subordinate units used TACWEB to access password protected forms allowing them to submit reports including the commander's assessment report,

patrol summary report, de-mining summary report, Personnel Daily Situation Report, logistic status, communications status, priority information requests (PIR), intelligence summaries, significant events, route and bridge status, spot reports, unexploded ordnance (UXO) reports and others. Staff elements used other forms to provide a variety of staff products. The staff provided G1 personnel roll-up, G3 operational focus, implementation instructions, commander's critical information requirements (CCIR) report, significant events, Joint Visitors Bureau report, staff comments, and others. The reports and staff products were viewed by browsing the websites.

Technically, the websites were built from unit reports and staff products dynamically over the MERCURY net. The units and staffs used input forms developed with Cold Fusion® and hyper-text markup language (HTML) with embedded structured query language (SQL) commands. Upon submission, the information uploaded to a SQL Server® database. Throughout the coalition, information was accessed on the websites using Microsoft Internet Explorer hyperlinks and viewing output forms or running a query on a specific subject. The output forms used Cold Fusion®, HTML, JAVA scripts and embedded SQL commands to query the database and display the information as web pages. Also, staff elements used Microsoft Front Page® to upload staff pages that contained information relevant to their functional area of expertise.

- Some of the improved capabilities this brought to MND(N) include:
- Adaptable to changes in mission or report formats
- Only need a web browser to access the information
- Easily accessed with a web browser from other networks that are physically connected
- Search Engines allows searches of archived historical information
- Battle Update Brief is built dynamically; briefed from the web
- Interfaces with other systems such as Balkan Digitization Initiative and ASAS remote work stations
- Patrols displayed on maps
- Build new reports; data fields easily added or modified
- Can import/export data with other databases to include Oracle® and others
- Reduced train-up time because most personnel are familiar with a web-based interface
- Uses little bandwidth since information is primarily text

- Releasable to Joint/Coalition units as long as the data is releasable

TACWEB was not without limitations. Some of these limitations included:

- Required a programmer/web developer with knowledge of Cold Fusion® and SQL Server® to change/modify reports
- Network problems can affect availability of the website
- Passive system: required personnel to pull information from the web
- No automated IDM function

LESSONS FROM OPERATION JOINT FORGE

Operations evolve over time and the command and control reporting systems mature. As complicated as the reporting applications are in the U.S. Army, adding coalition partners further complicates the interoperability issues. The expensive, proprietary software of the stove-piped systems often require specific platforms and are usually not releasable to allies or coalition partners. But information sharing is imperative for effective command and control.

With TACWEB, the commander could refine his information requirements as the mission evolved. As new information was needed to support particular operations, new reports were developed and new displays programmed. The data was added to the database and was available for query even after the operation was completed. While nations retain the logistical support responsibilities, command and control of coalition partners can be greatly improved with an adaptable, web-based reporting system. The flexibility of being able to change report formats to suit particular missions increases its utility across the full spectrum of operations and as requirements evolve.

The most important lesson from this operation was the way the commander taught his staff what information was important. In daily, interactive discussions, the commander was able to explain what he needed to build his mental image of a particular situation. The staff responded by learning to anticipate the commander's needs and more importantly, his follow-on questions. They then could provide most of the information in the initial discussion, eliminating the time delay required with follow-up. Understanding how the commander thinks and processes information is just as important as the basic data. As one Chief of Staff put it, "do not just put a bunch of data points on the wall for the boss. Connect the dots and color in the picture."

JOINT VISION 2020: NETWORK CENTRIC WARFARE

"While the nature of war remains constant, the conduct of war is continually undergoing change in response to new concepts, technologies, and capabilities. How armed forces adapt to such changes determines their readiness to confront future operational challenges and threats."[9] One of the objectives of the current military transformation is to harness the power of information sharing in networks. The speed of processing and the technological breakthroughs are accelerating. Harnessing these changes and exploiting them for military use could exponentially improve all aspects of operations, from planning to deployment to execution, through transition and redeployment. That is why the joint vision focuses on networking everything from national intelligence assets to sensors in theater to weapons platforms and dismounted soldiers. This concept, as illustrated below, is called "Network Centric Warfare."

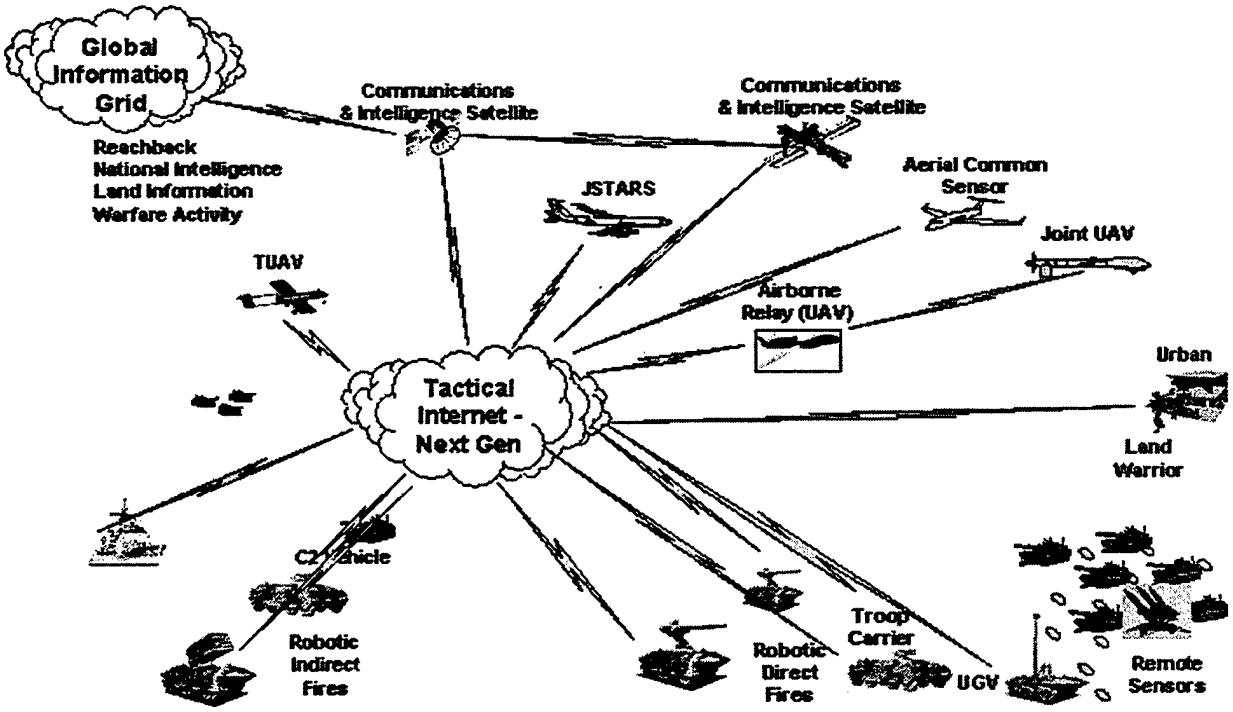

FIGURE 4: NETWORK CENTRIC WARFARE[10]

An example at the tactical level may explain this better. The focus at this level is to "...see first, act first and finish decisively...."[11] Picture sensors on unmanned vehicles (UAV, UGV), in space, in the air, and on the ground all sending real time data over the network; data fusion

without human intervention; and a common operating picture of the enemy available to the soldiers and leaders simultaneously. Some of this information is also fed simultaneously to weapon systems capable of line-of-sight and beyond line-of-sight target acquisition. Once leaders decide which targets to engage, the continuous update of information allows the weapons to engage the target precisely. The concept plans to capitalize on the synergistic effects of shared information to accelerate precision engagements.

THE GLOBAL INFORMATION GRID

This network centric environment envisioned for future operations has led to the development of a C4 infrastructure concept called the Global Information Grid (GIG). It is defined as

> the globally interconnected, end-to-end set of information capabilities, associated processing, storing, dissemination and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing services, software (including applications), data, security services and other associated services necessary to achieve Information Superiority...The GIG supports all Department of Defense, National Security, and related intelligence community missions and functions (strategic, operational, tactical, and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms and deployed sites). The GIG provides interfaces to coalition, allied, and non-DOD users and systems.[12]

Simply put, from the strategic level to the deployed tactical level, whether in the air, or on the sea or land, the grid of telecommunications networks that handle, transport, and process information should be almost transparent to the user. Once entered by the supplier, information will be dynamically routed to the consumer and secured throughout its life cycle.

JP 6-0 explains how the GIG is envisioned to meet the information superiority needs of the commander by breaking the GIG into seven basic components: warrior, global applications, communications, computing, foundation, network operations, and information management. The first four components constitute the hardware, software, and applications portion of the GIG: it is the technology-driven portion. The fifth component, foundation, is the doctrine, training, standards, policy and engineering to implement the GIG. The last two components are focused on managing the GIG: the information management and network operations components. The tools to facilitate these two key portions of the GIG have been technologically enhanced, but the key functions have existed as long as there have been communications and data networks.

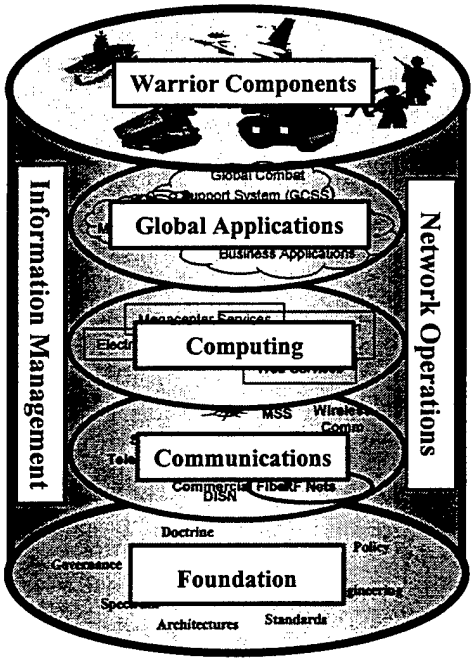

FIGURE 5: THE GIG[13]

The warrior component provides information on demand to the network centric shooter platforms including the sensors and targeting for fire support, and the battle damage assessment. This is the "customer" level of the GIG. It is due to the interoperability and connectivity at this level that the GIG is essentially part of the weapon systems. The current theater missile defense system is a good example of the sensor to shooter connectivity envisioned for ground and sea platforms in the future. The sensors that acquire a target are all linked and a common relevant operating picture is simultaneously and continuously transmitted to the air, ground and sea platforms capable of engaging targets. It has taken over a decade to work out all the interoperability details in this one system, but it proves that it is feasible.

The global applications layer focuses on systems for key functions for joint forces such as command and control, medical, logistical, or weather. Some of the currently fielded systems include the Global Command and Control System (GCCS), Global Command Support System (GCSS), and Theater Battle Management Core System (TBMCS).[14] Ensuring all these

applications are completely interoperable (fully capable of data sharing) is a major challenge and is critical. The GCCS and GCSS were designed to work together but there are hundreds of other systems in the Department of Defense (DOD) that are all "stove-piped," or only have connectivity to others within their functional community. The next two figures illustrate the difference between marginally interoperable "stove-piped" systems and the vision for applications of the future.

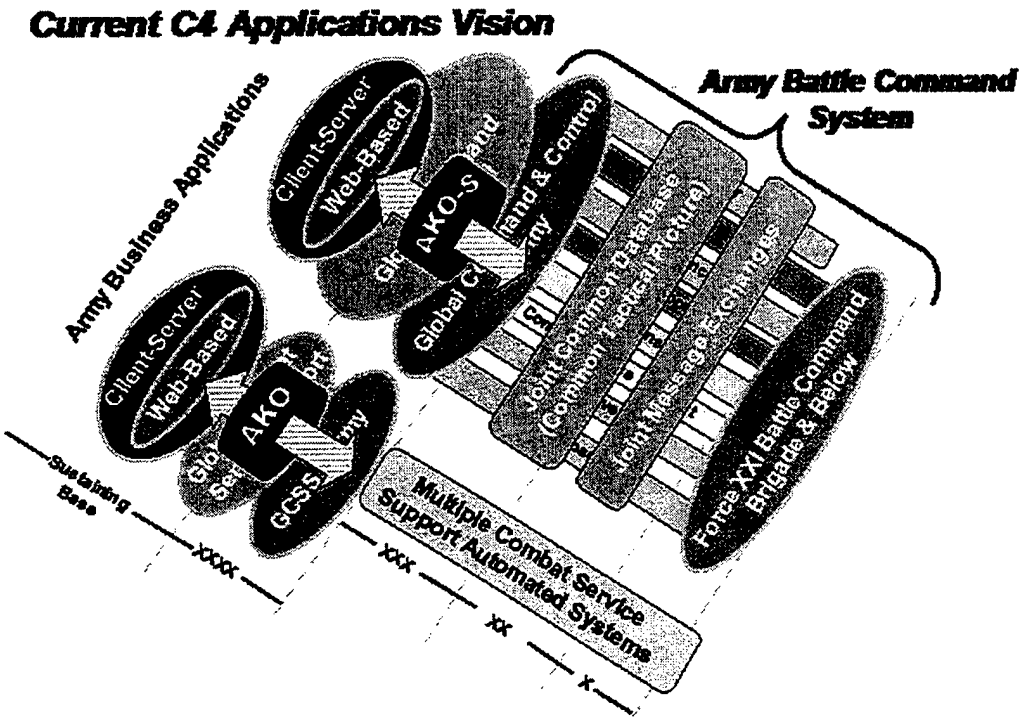

FIGURE 6: CURRENT C4 APPLICATIONS[15]

The Army Battle Command System (ABCS) consists of several applications that are designed to share certain pieces of data with the GCCS (Army). They are also designed to input data to the Joint Common Database and they can exchange messages through the Joint Message Exchange. Notice that the combat service support systems run parallel and only share data through the GCSS.

In contrast, the future applications are envisioned to be built on open architectures, inputting and retrieving data from a common database, or data warehouse. Here the units of action and employment (UOA, UOE) have equal access to information across the functional areas.

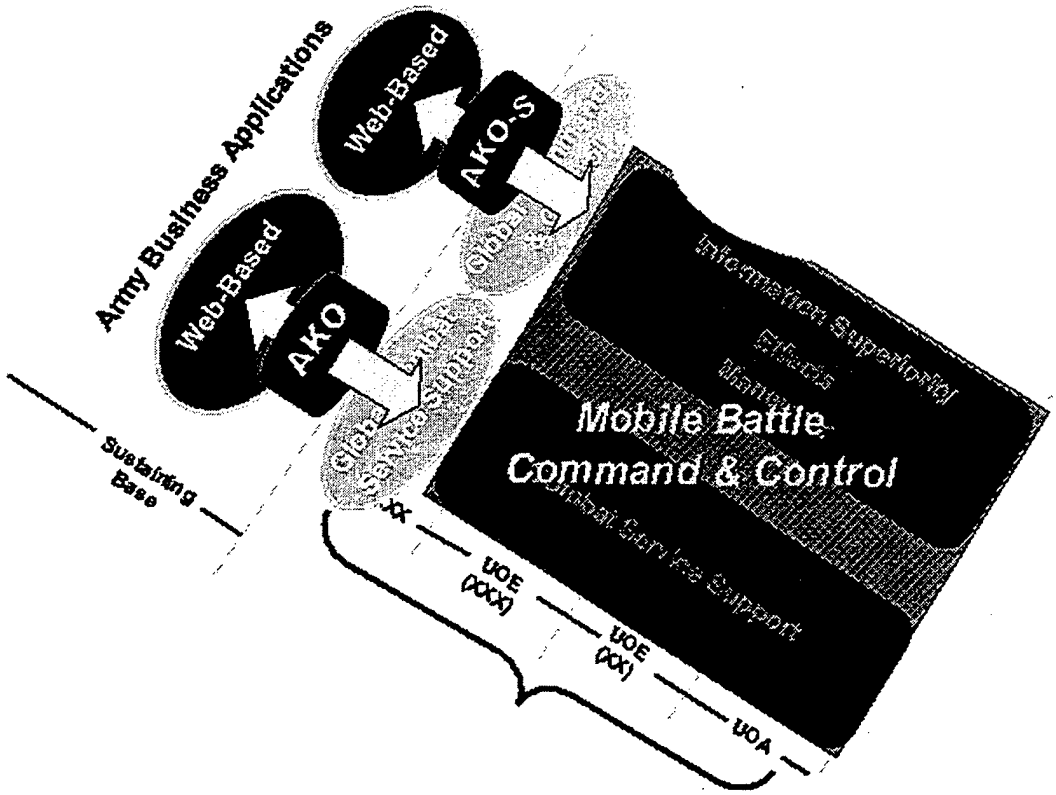

FIGURE 7: FUTURE C4 APPLICATIONS[16]

The computing component is designed to facilitate the data sharing across all the interoperable communities. It includes the hardware, software, data warehouses and web services. The Defense Information Systems Agency (DISA) has the lead in developing and implementing a computing infrastructure to service all the DOD. They also develop the technical architectures that define standards for all data networks. The personal computing component continues to include all networked computers worldwide. The current initiative within DOD to consolidate all servers will improve both interoperability and security.

The communications component consists of all the "pipes" the data flows through; from bases to the field, sea, or air. It is made up of all the integrated systems in the Defense Information System Network (DISN) extending to the tactical level. The majority of the DISN currently relies on satellite communications. The vision for the future includes moving many of the long-term circuits from the satellites to fiber optic, or other terrestrial based system, and redirecting satellites for increased flexibility into the deployed theater.[17]

A recent DOD initiative demonstrated how the network might be implemented for the ground soldier. The Extending the Littoral Battlespace Advanced Concept Technology Demonstration conducted last summer installed a wireless, digital network linking tactical units with each other and with the ships off shore. Called the Wide Area Relay Network (WARNET), it clearly demonstrated that the soldiers at the tactical level could access critical information on the move.[18] It combined the use of shared data with the flexibility of satellite communications to improve the situational awareness of leaders fighting in a complicated environment.

The information management component focuses on ensuring warfighters around the world have access to key data. It is evolving into more of a "knowledge management" function which focuses on "handling, directing, governing, or controlling of natural knowledge processes...." [19] Knowledge is the process of taking information and putting it in context. Joint Forces Command is experimenting with a software program from TheBrain Technologies Corporation in order to "integrate, visualize and manage information."[20] This software "provides real-time access across various applications and integrates this information across many different sources."[21]

The network operations component must provide "seamless end-to-end management of networks, global applications, and services across the GIG...."[22] It is broken down into network management, information assurance, and information dissemination management. Network management is the planning, implementation and controlling of the network. Responsibility for managing specific portions of the network is delegated by DISA or theater Commanders. "Having end-to-end awareness of the networks comprising the GIG and then properly managing those networks from the strategic to the tactical level, ... plays a critical part of synchronizing our forces in peacetime or war." [23] Network management functions consist primarily of connectivity, bandwidth allocation, rerouting and technical management of the contingency networks.

Information Assurance is the function designed to protect and defend our systems and the data within them in order to provide the continuous information needed to gain and maintain information superiority. It includes the detection of an attack, as well as the response and restoration after any attack. Attacks to the GIG may be intentional or accidental but the results can be equally catastrophic. Increased interoperability and integration can lead to increased vulnerabilities. This particular function has received a significant amount of attention and efforts in the past three to five years, yet vulnerabilities still exist and with the continuous evolution of technology, new opportunities for assault emerge. The Defense in Depth[24] program raised user awareness through proper training in tactics, techniques, procedures and policy.

Information dissemination management focuses on "providing the right information to the right place at the right time over the right communications path."[25] It includes both the technical challenges of managing information and the determination of the information requirements. It will require an information manager at each level of an organization in order to make this vision a reality.

INFORMATION DISSEMINATION MANAGEMENT

> The principle shortfall IDM addresses is the lack of integrated, cross functional capabilities to manage information dissemination. This has resulted in reduced access, awareness, and in some cases, delivery of information required by the Warfighter. Existing information systems capabilities are primarily stovepipe solutions operating either within a single service or functional area, a single area of responsibility, or a single domain. Specific shortfalls include: limited user awareness and access to needed information; the lack of defined, automated, and prioritized user information needs; and limited means to adjust the flow of information from producers to users.[26]

The concept of information dissemination management for the future GIG begins with understanding the commander's requirements and guidance. The intent is to provide an uninterrupted flow of information and to be able to dynamically change delivery priorities based on the commander's priorities throughout an operation. This can only be accomplished through the key elements of information awareness, access, and delivery. It involves the compilation, cataloging, caching, distribution, and retrieval of data.

Quite often the issue is not that the information is not available somewhere. The problem is that the commander (or his staff) does not know where or how to get the information; does not have access, due to security or technological reasons; or the information arrives too late or in an unusable form. Therefore all the IDM functions are designed to either: "increase access to information, increase awareness of information, increase delivery of that information, or enhance the commander's ability to control information dissemination within the area of operation." [27]

The IDM Capstone Requirements Document was approved in January 2001, giving DISA the lead in developing the IDM tools for the DISN down to theater level. The solutions under development are a combination of current commercial off the shelf and government off the shelf software plus some still under development. The entire suite, when completed, seeks to fulfill all the functional capabilities listed in the table below with the primary objective of improving information flow.

AWARENESS	ACCESS	DELIVERY	SUPPORT SERVICES
Cataloging	Profile Manager	Retrieval	Security
Searching	Policy Manager	Resource Monitoring	Directory services
Advertising		Delivery planning	Catalog Management
			Operations

TABLE 1. FUNCTIONAL CAPABILITIES OF IDM

The three functions of cataloging, searching, and advertising should improve users awareness of the availability of specific information, even unstructured data. It also allows the user to build a profile of information needs and automatically find the needed information. The information manager then uses the profile manager function to establish priorities of users or information and the delivery planning function to establish policies within and between domains.[28]

While the mission profiling and policy manager pieces of the software are still in the developmental phase, most of the software associated with IDM awareness, access, and delivery are completed and will be field-tested in Pacific Command later this year.[29] This software will greatly facilitate the management of the information when fully fielded.

SITUATIONAL UNDERSTANDING FROM DATA CHAOS

Joint Vision 2020 is network centric warfare dependent upon the Global Information Grid to facilitate the timely sharing of information. Information Dissemination Management is designed to establish priorities for information and facilitate its timely delivery. All the doctrine development and technological efforts are focused on ensuring the information gets to the right place at the right time. The concept of IDM even states that it begins with understanding the commander's requirements but stops short of explaining HOW the J6 is supposed to accomplish this. SO, where are the efforts at ensuring that it is the RIGHT information?

Almost every military school addresses this challenge by teaching a procedure. The Army Intelligence School has the most detailed process called the Intelligence Preparation of the Battlefield (IPB). This step-by-step procedure walks the officer through an analysis of all the major factors affecting the outcome of the battle: weather, enemy order of battle, terrain, etc. What is missing in most of these procedures or models is what frustrates commanders: the lack of analysis showing relevancy.

> A new Information Revolution is well under way. It has started in business enterprise, and with business information. But it will surely engulf ALL institutions

> of society. It will radically change the meaning of information for both enterprises and individuals. It is not a revolution in technology, machinery, techniques, software or speed. It is a revolution in CONCEPTS....So far, for fifty years, Information Technology has focused on DATA – their collection, storage, transmission, presentation. It has focused on the "T" in "IT." The new information revolutions focus on the "I." They ask "What is the MEANING of information and its PURPOSE?"[30]

What is missing today is the step beyond these procedures and information models: the thinking and processing of the information. JTF staff officers and subordinate commanders must be able to conceptualize the mission and understand the commander they support in order to properly define the information requirements. It is not enough for the staff to simply provide data bits to the commander: they have to understand the meaning and purpose of the information. The staff needs to put the information into context of the situation and analyze the information by answering questions such as:

1. Why does the commander need to know this?
2. When does the commander need this information?
3. What is the commander going to do with this information?
4. What other information is related to this information and how?
5. How does this information impact current operations?
6. How does it impact future operations?
7. What is the impact on a decision if the commander does not get this information?
8. Who else needs to know? When?
9. How does this information contribute to the commander's image of the situation?
10. What is the best way to express or portray this information?

Answering these questions helps to put the information in context and, with the help of all the automated tools discussed previously, begins the process of converting information into knowledge: knowledge the commander needs to make the critical decisions. If the future warfighting commander is going to get in front of the adversary's decision cycle and stay there, he will need all the technological advantages the joint vision espouses. But to truly reach situational understanding, he will need all the technology plus a staff capable of providing him the analyzed information he needs. The right information at the right time at the right place starts with the right information.

CONCLUSIONS

The concepts for warfighting in the future rely upon commanders with better situational understanding making critical decisions quicker than the enemy can react. This decision superiority is enabled by the global information grid providing the right information to the commander at the right place and time. Concerted efforts by the entire joint communications and intelligence communities are focused on ensuring that the technical aspects of communications, computer applications, data sharing, and end user platforms are fully interoperable. Defining the operational and technical architectures is almost complete. DISA leads the charge with Joint Forces Command and Pacific Command testing concepts and products as they become available.

But the most critical step in information dissemination management is the first one: defining the commander's information requirements. And the issue gets more complicated in network centric warfare. Currently, the staff and commanders are limited by what information is available on their stove-piped system. The information delivered is a function of the architecture and system designs. However, the information available grows exponentially when everything is networked and everyone has access to almost unlimited data across functional domains. The critical role for information managers becomes properly defining the information requirement versus simply providing an architecture for the systems to communicate across.

Unless equal attention and efforts are put into this part of the equation, the military could find itself with better technology and fail in providing the commander the information he requires to make the critical decisions. Simply providing more information to the commander is not the way to achieve decision superiority. Commanders cannot, by themselves, process all the information provided to them. Staffs must move beyond set procedures and think about the actual meaning of information. They need to be able to analyze it and put it in the context of the current and future situation and present the commander with a more complete understanding of the situation. Only then can commanders achieve decision superiority.

WORD COUNT = 6923

ENDNOTES

[1] Henry H. Shelton, Joint Vision 2020 (Washington, U.S. Joint Chief of Staff, 2000) 2-11.

[2] Robert H. Scales, America's Army in Transition: Preparing for War in the Precision Age, Army Issue Paper No.3, (Carlisle: Strategic Studies Institute, 1999), 12.

[3] James P. Kahan, D. Robert Worley, and Cathleen Stasz, Understanding Commanders' Information Needs (Santa Monica: RAND Corporation, 1989), 87-94.

[4] Ibid.

[5] JV2020.

[6] Ibid.

[7] U.S. Department of Defense, Joint Doctrine for Employment of Operational/Tactical Command, Control, Communications, and Computers (C4) Joint Publication 6.-02,(Washington D.C.: U.S. Department of Defense, 1996), I-1.

[8] Ibid.

[9] Eric Shinsecki, "Concept for the Objective Force," 2001.

[10] Peter Zielinski, "United States Army White Paper: Concepts for the Objective Force," briefing slides with commentary, USAWC, February 2002.

[11] Ibid.

[12] U.S. Department of Defense, Doctrine for Command, Control, Communications, and Computers (C4) System Support to Joint Operations Joint Publication 6.0 DRAFT,(Washington D.C.: U.S. Department of Defense, 2002), II-1

[13] JP 6.0, II-5.

[14] TBMCS is a set of 54 applications providing planning, execution, and intelligence processing for the air campaign. Sixteen of the applications are used by all the services.

[15] Objective Force Task Force, "Transforming to the Objective Force," briefing slides with commentary, provided on CD-ROM to USAWC, 28 January, 2002.

[16] Ibid.

[17] John P. Cavanaugh, "Signal Regiment Vision 2020: Transforming the Regiment in the New Millennium," briefing slides with scripted commentary, Fort Gordon, U.S. Army Signal Center, 10 December 2001.

[18] Ray Cole, "Networking the Battlespace: DOD Technology Demonstration extends C3I Connectivity Down to the Squad level." Armed Forces Journal, (July 2001), 36.

[19] JP 6.0, II-26.

[20] "Information Plus Context Equals Knowledge," Signal, (February 2002), 37.

[21] Ibid., 38.

[22] JP 6.0, II-16.

[23] Ibid.

[24] The Defense in Depth program focuses on defense from the user through the network. It emphasizes education, certification, and awareness.

[25] Ibid.

[26] JP 6.0, II-18.

[27] Ginny Parsons, "Information Dissemination Management (IDM) Overview," briefing slides with scripted commentary, Defense Information Systems Agency, Washington D.C., 21 December 2001.

[28] Ibid.

[29] Timothy M. Petit, Robert Lietze, and Mark Miller, "Partnerships – The Key to Success for Pacific Theater Network Operations (NETOPS)," IANewsletter, (Winter 01/02), 12.

[30] Peter F. Drucker, Management Challenges for the 21st Century, (New York: Harper Collins Publishers, 1999), 97.

BIBLIOGRAPHY

Becker, Mark A. Command and Control in a Joint Operational Environment: The Hybrid Control Maxim. U.S. Naval War College, Joint Military Operations Department, 8 February 2000.

Cavanaugh, John P. "Signal Regiment Vision 2020: Transforming the Regiment in the New Millennium." Briefing slides with scripted commentary, Fort Gordon, U.S.Army Signal Center, 10 December, 2001.

Cesar, Edison M. Strategies for Defining the Army's Objective Vision of Command and Control for the 21st Century. Santa Monica: RAND Corporation. 1995.

Cole, Ray. "Networking the Battlespace: DOD Technology Demonstration extends C3I Connectivity Down to the Squad level." Armed Forces Journal, (July 2001): 36.

Drucker, Peter F. Management Challenges for the 21st Century. New York: Harper Collins Publishers. 1999.

Fonesca, Brian. "Pioneers push app Distribution Alternatives." Infoworld, No. 23 (March 12, 2001): 33.

Kahan, James P., D. Robert Worley, and Cathleen Stasz. Understanding Commanders' Information Needs. Santa Monica: RAND Corporation, 1989.

Kust, Peter Nayland. "Information Overload: IT Managers must focus to bring order out of chaos." Infoworld, no. 21, (February 8, 1999): 62.

Owens, William A. Lifting the Fog of War. New York: Farrar, Straus and Giraux, 2000.

Parsons, Ginny. "Information Dissemination Management (IDM) Overview." Briefing slides with scripted commentary, Defense Information Systems Agency, Washington D.C., 7 December, 2001.

Petit, Timothy M., Lietze, Robert, and Miller, Mark. "Partnerships- The Key to Success for Pacific Theater Network Operations (NETOPS). IA Newsletter 4 (Winter 01/02): 12-17.

Scales, Robert H. America's Army in Transition: Preparing for War in the Precision Age, Army Issue Paper No.3. Carlisle: Strategic Studies Institute. 1999.

Shalikashvili, John M. Joint Vision 2010. Washington D.C.: U.S. Joint Chiefs of Staff, 1996.

Shelton, Henry H. Joint Vision 2020. Washington D.C.: U.S. Joint Chiefs of Staff, June 2000.

U.S. Army Objective Force Task Force. "Transforming to the Objective Force." briefing slides with commentary, provided on CD-ROM to USAWC, 28 January, 2002.

U.S. Department of Defense, Doctrine for Command, Control, Communications, and Computers (C4) System Support to Joint Operations Joint Publication 6-0 DRAFT. Washington D.C.: U.S. Department of Defense, 2002.

U.S. Department of Defense, Doctrine for Employment of Operational/Tactical Command, Control, Communications, and Computers (C4) Systems Joint Publication 6-02. Washington D.C.: U.S. Department of Defense, 1996.

Zielinski, Peter. "United States Army White Paper: Concepts for the Objective Force." Briefing slides with commentary, presented to Course 800, USAWC Carlisle Barracks, February 2002.