AD NUMBER

ADB349930

LIMITATION CHANGES

TO:

Approved for public release; distribution is unlimited.

FROM:

Distribution authorized to U.S. Gov't. agencies only; Administrative/Operational Use; MAY 2006. Other requests shall be referred to US Army War College, Carlisle Barracks, PA 17013-5050.

AUTHORITY

USAWC ATWC-AA ltr dtd 16 Dec 2009

Strategy Research Project

IMPEDING NETWORK CENTRIC WARFARE: COMBATANT COMMAND INFORMATION TECHNOLOGY SUPPORT

BY

COLONEL DAVID A. BARLOW
United States Army

USAWC CLASS OF 2009

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

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

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
28-02-2009	Strategy Research Project	

4. TITLE AND SUBTITLE

Impeding Network Centric Warfare: Combatant Command Information Technology Support

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Colonel David A. Barlow

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

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

Jeffrey L. Groh, D.Sc.
Department of Distance Education

8. PERFORMING ORGANIZATION REPORT NUMBER

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

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

10. SPONSOR/MONITOR'S ACRONYM(S)

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

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution A: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Network centric warfare is the method used by the United States combatant commands to wage war. Information technology is a fundamental enabler of network centric warfare. The ten combatant commands use different methods to provide desktop information technology support to their staffs. The result is different sets of applications, capabilities, and business processes that impede collateral information sharing between commands, Services, and the Department of Defense. Unimpeded information sharing is a central tenet of network centric warfare. The different combatant command information technology support methods impede network centric operations within the Department of Defense.

This paper examines desktop collateral information technology support to the combatant commands as it pertains to network centric warfare at the theater level. It proposes a single solution provided by a single agency to service all ten combatant commands. It examines the strengths and weaknesses of the current support methods and the proposed solution. Based on this study, the paper provides strategic recommendations aimed at improving network centric warfare.

15. SUBJECT TERMS

Information Sharing, Self-synchronization, Shared Awareness

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	30	

USAWC STRATEGY RESEARCH PROJECT

IMPEDING NETWORK CENTRIC WARFARE: COMBATANT COMMAND INFORMATION TECHNOLOGY SUPPORT

by

Colonel David A. Barlow
United States Army

Jeffrey L. Groh, D.Sc.
Project Adviser

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

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

ABSTRACT

AUTHOR: Colonel David A. Barlow

TITLE: Impeding Network Centric Warfare: Combatant Command Information Technology Support

FORMAT: Strategy Research Project

DATE: 28 February 2009 WORD COUNT: 5681 PAGES: 30

KEY TERMS: Information Sharing, Self-synchronization, Shared Awareness

CLASSIFICATION: Unclassified

Network centric warfare is the method used by the United States combatant commands to wage war. Information technology is a fundamental enabler of network centric warfare. The ten combatant commands use different methods to provide desktop information technology support to their staffs. The result is different sets of applications, capabilities, and business processes that impede collateral information sharing between commands, Services, and the Department of Defense. Unimpeded information sharing is a central tenet of network centric warfare. The different combatant command information technology support methods impede network centric operations within the Department of Defense.

This paper examines desktop collateral information technology support to the combatant commands as it pertains to network centric warfare at the theater level. It proposes a single solution provided by a single agency to service all ten combatant commands. It examines the strengths and weaknesses of the current support methods and the proposed solution. Based on this study, the paper provides strategic recommendations aimed at improving network centric warfare.

IMPEDING NETWORK CENTRIC WARFARE: COMBATANT COMMAND INFORMATION TECHNOLOGY SUPPORT

The different information technology support methods used by the ten United States combatant commands impede network centric operations within the Department of Defense. Network Centric Warfare (NCW) is the method used by the combatant commands to wage war. Information technology is a fundamental enabler of network centric warfare. The ten combatant commands use different methods to provide desktop information technology support to their headquarters staffs. The result is different sets of applications, capabilities, and business processes that impede information sharing between commands and the Department of Defense (DoD), and sometimes between a combatant command and its own components. Information Technology (IT) support at the combatant commands, meant to be a NCW enabler, often fails to support information sharing.

Unimpeded information sharing is a central tenet of network centric warfare.[1,2] The current disjointed IT support methods at the combatant commands impede information sharing within and between the commands. This lack of seamless information sharing does not support NCW, and interferes with the combatant commands' synchronization of the elements of national power. Through examination of several of the IT applications meant to facilitate information sharing, this paper will demonstrate the important role combatant command desktop IT support plays in NCW. The joint, interagency, intergovernmental, and multinational (JIIM) nature of the current and future operational environment[3] impose a huge information sharing requirement on the combatant commands. Developing NCW capabilities to better enable the

combatant commands to synchronize the elements of national power will require the DoD to fundamentally change the way in which it provisions IT support at the combatant commands.

This paper addresses secret collateral and below IT support, commonly known as “SIPRNet” (Secret Internet Protocol Router Network) and “NIPRNet” (Non-classified Internet Protocol Router Network) services. The Joint Worldwide Intelligence Communications System (JWICS), while fundamentally an IT system, is provisioned through the Defense Intelligence Agency (DIA). DIA provisions JWICS support separately and distinctly from the organizations that provision collateral IT services at the combatant commands.

This paper examines desktop collateral information technology support to the combatant commands as it pertains to network centric warfare at the theater level. It proposes a single solution provided by a single agency to service all ten combatant commands. It examines the strengths and weaknesses of the current information technology support methodology and the proposed solution. Based on this study, the paper provides strategic recommendations aimed at improving the network centric warfare capabilities across the combatant commands.

Background

The United States combatant commands exist to provide command and control of the broad array of forces and functions that the individual Services and Defense Agencies can provide.[4,5] The doctrinal framework in which the combatant commanders assert their command and control has become Network Centric Warfare (NCW).[6]

In its most basic form, NCW seeks to achieve increased agility and effectiveness when compared to industrial age warfare. NCW first requires shared awareness. People and systems normally achieve shared awareness through information sharing. NCW practitioners then leverage this shared awareness to achieve a greater degree of self-synchronization. The emergence of self-synchronizing behavior is the core of the power of NCW, leading directly to increased agility and effectiveness.[7] Within the context of IT support at the combatant commands, self-synchronizing behavior automates many internal and external staff functions, reduces administrative work, improves generation of information from data, and increases staff responsiveness. This increased staff responsiveness could take the form of faster decision making, more time for conceptual thinking, or a combination of both.

The DoD intends its "plug and play" information infrastructure[8] to tie together all of the information generation and analysis assets that fall under the command and control of the combatant commanders. This infrastructure enables the shared awareness that NCW requires. This same infrastructure serves as the conduit of self-synchronization at all levels. The physical instantiation of the DoD information infrastructure at any particular combatant command headquarters is comprised of a set of information technology (IT) systems and supporting personnel. The IT systems and support that are the subject of this paper comprise the "last mile," quite often literally, of the DoD information infrastructure.

The DoD provisions IT support at the combatant commands through a multi-tiered system, shown in Figure 1. The Secretary of Defense, through the Assistant Secretary of Defense Networks and Information Integration (NII)/DoD Chief Information

Officer (CIO), determines overall DoD IT policy. The OSD(NII)'s stated mission is to "enable net-centric operations."[9] The Defense Information Systems Agency (DISA) works for OSD NII and is responsible for the Global Information Grid (GIG), a broad-band telecommunications network and associated services. The GIG is similar in nature to a commercial IT services provider when viewed from a computer networking perspective.

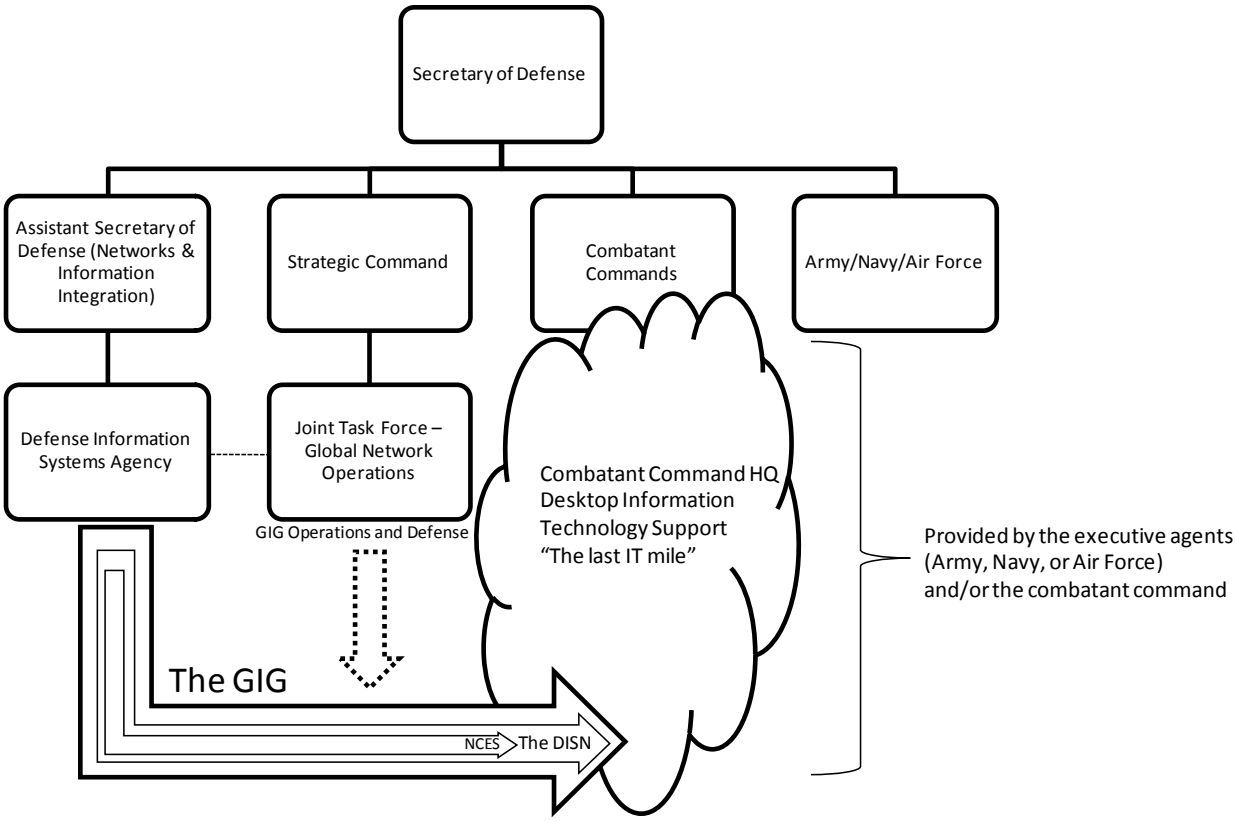

Figure 1. DoD Organization for IT Support at the Combatant Command Headquarters

The data transport portion of the GIG is the Defense Information Systems Network (DISN). The GIG/DISN provides "points-of-presence" at various DoD locations, including all combatant commands, for high-speed network services access. DISA funds DISN services through a Defense Working Capital Fund (DWCF), with the

Services paying for most of the combatant commands' DISN support.[10] DISA, via the GIG/DISN, provides NCW-enabling enterprise-level software services - collaboration tools - to all DoD network users. DISA calls this program "Network Centric Enterprise Services" (NCES). These NCES replace individual combatant command collaboration tools that have limited or no interoperability and tenuous funding. The NCES tools enable network-centric collaboration across all DoD elements, including the combatant commands. NCES has freed all DoD elements, including the combatant commands, from having to operate and maintain (and fund in many cases) their own fundamentally non-network centric sets of collaboration tools.

Joint Publication 1, "Doctrine for the Armed Forces of the United States", states that US Strategic Command (STRATCOM) has responsibility to "plan, integrate, and coordinate DOD global network operations"[11] STRATCOM does so through the Joint Task Force – Global Network Operations (JTF-GNO).[12] The commander of DISA is dual-hatted as the commander of JTF-GNO.[13]

The desktop IT support considered in this paper is the user interface to the GIG; the "last IT mile" between the GIG/DISN and each IT user. This "last IT mile" is extremely important to NCW as much of the information that combatant commands' utilize is created, manipulated, and stored by the various "last IT mile" systems connecting the GIG/DISN to the combatant commands' desktops.

Desktop IT support at a combatant command headquarters is the purchase, installation, operation, and maintenance of hardware and software systems to support the business processes of that headquarters. This IT support encompasses all user devices such as the desktop and laptop computers and the software on those

computers. It also includes cellular devices and software used to provide mobile email and Internet access. The local network infrastructure is part of desktop IT support. This infrastructure includes server rooms with associated servers and support infrastructure, most software run on the servers in the server room(s), 24x7 help desk services, and the logistics system that supports every IT item, cradle to grave. The level of support required is significant – meeting the 24x7, high-reliability IT requirements of the combatant commander and his staff is an extremely demanding mission. Likewise, the cost is significant – in the neighborhood of $25 million annually per combatant commander when a contractor provides the support.

As a primary enabler of NCW, IT support has become ever more vital to the functioning of the national defense. As computer networking developed in the 1990's, desktop IT support struggled to keep pace, particularly from an organizational perspective. The Services each developed their own methods to provide this support, only modestly unified by the common hardware (IBM-PC architectures), operating system and office productivity software (Microsoft products), and the TCP/IP protocol. In all the Services, desktop IT support started as a small-unit activity. IT systems were not standardized from any perspective. Over time, each Service has adopted a much more centralized approach. The Navy has completely contracted out their desktop IT support to a single contractor. The Army and the Air Force each use a combination of contractors, service personnel, centralized provisioning, and standards to provide their versions of desktop IT support. The Services' motivation for central and standard solutions has been driven much more by lack of resources than enhancing NCW capabilities. However, these central and standard solutions have enhanced the

Services' NCW capabilities. From the desktop IT support perspective, these enterprise solutions better enable information sharing and improve the potential for self-synchronization within the Services.

The DoD assigns each combatant command a Service as its executive agent.[14] The Service, as executive agent, has numerous responsibilities, including provisioning of IT support.[15] For each combatant command, the executive agent's provisioning of IT support is accomplished unique to that command, primarily influenced by the executive agent's IT support system. Executive agent control of IT support funding, or lack thereof, has also influenced the wide spectrum of IT support methods employed at the combatant commands.

There are several DoD Directives[16] that deal with information technology. None of the directives specifically address desktop IT support. Their perspective is strategic, yet their direction applies quite specifically to the "tactical" problem of provisioning desktop IT support at the combatant commands' headquarters. Several of these directives address constructing and enabling a network centric DoD. All of them apply direction at the enterprise level, raising but not addressing the question: Is the DoD and Joint Community, comprised mainly of the combatant commands, an "enterprise?" A network-centric approach to warfare would seem to require the answer to be a resounding "yes!" Yet given the current desktop IT support situation, there is certainly not such an enterprise – particularly when it comes to data and information management.

The DoD Directive "Management of DoD Information Resources and Information Technology," serves as the capstone DoD information system directive. While it does

not directly address combatant command IT support, it does direct DoD Components to use DoD-wide automated information systems and software.[17] This Directive, along with DoD Directive "IT Portfolio Management,"[18] require a level of IT management expertise and resources normally found only at organizations providing enterprise-level IT support. These organizations are few within the DoD -- DISA, the Services' communications commands, and the Defense Intelligence agency (DIA) are examples.

The DoD Directive "Data Sharing in a Net-Centric Department of Defense," mandates that DoD data be visible, accessible, understandable, and trustable; and by inference, retained for possible future use.[19] The implementing guidance for this directive clearly recognizes the magnitude and difficulty of implementing this mandate, explicitly breaking the implementation into "communities of interest" in an attempt to build this capability incrementally.[20] Additional direction on network centric data conformity, provided by DoD Directive 8320.03, mandates unique identification (UID) standards for "discrete entities." It infers that each combatant command is such a discrete entity.[21]

Joint doctrine does not directly address the provisioning of desktop IT support to the combatant commands. Joint Publication 6-0, "Joint Communications Systems," does not address combatant command headquarters IT support; the reader is left to infer that it is a combatant command J-6 responsibility.[22] The focus of Joint Pub 6-0 is on force projection communications and network operations, all supported by the Global Information Grid (GIG).

IT Support Methods

The differences in IT support methods at the ten combatant commands are well illustrated by examining the extremes. On one end of that spectrum is the Navy-provisioned support of Pacific Command (PACOM) and on the other end is the "do-it-ourselves" approach of European Command (EUCOM). The two commands have many similarities. Both are geographic combatant commands (GCC), responsible for engagement with large numbers of countries spread over large geographic areas. Both have assigned forces through their component commands, and both have been in existence since the end of World War II. The executive agent for PACOM is the Navy, while the executive agent for EUCOM is the Army.

The Navy provides IT support to PACOM via the Navy Marine Corps Intranet (NMCI). NMCI is a consolidated, enterprise approach to providing IT support to Navy and Marine Corps forces, activities, and supported commands such as PACOM. At end state, NMCI will support over 700,000 users with standard sets of hardware and software services.[23] NMCI is a multi-year contracted effort costing several billion dollars, and has been the subject of considerable congressional scrutiny. It has suffered from most issues that large enterprise-wide projects tend to incur – particularly projects focused on satisfying the needs of hundreds of thousands of customers.[24] The IT Services Division in the PACOM J6 provides the staff interface between the PACOM staff and NMCI; NMCI staff manages all the IT hardware, software, and network operations. Headquarters PACOM business processes and/or technical requirements that require changes to the NMCI standardized solution(s) must be implemented in such a way that all NMCI users remain supported and all security requirements remain satisfied. In practice, customization of enterprise IT systems is a difficult task both

administratively and technically. Therefore, reaction time to user requirements that necessitate change is usually lengthy. This tends to force organizations to comply with existing network standards rather than pursue solutions that would require network changes.[25]

Although the Army is the executive agent for EUCOM, most of EUCOM's IT support is self-provided. Using an IT services contract provided and managed by the General Services Agency (GSA),[26] EUCOM has a task order that provides all aspects of IT support with the exception of the unclassified network infrastructure – cable, switches and routers provided and managed by the Army. A contractor provides all other IT support through the task order off the GSA contract. All the IT hardware, software, and network operations are managed directly by the Headquarters Enterprise Services Division in the EUCOM J6. Because the IT contractor responds directly to EUCOM's requirements, EUCOM's desktop IT services directly reflect the local requirements of the EUCOM Headquarters staff – i.e. they are customized and often have limited compatibility with components and other combatant command IT systems, from a business process perspective and/or a technical interface perspective.

NCW-Related Problems Created by IT Support Methods

The current combatant command HQ IT support methods significantly impede the NCW tenets of shared awareness and self-synchronization. Fundamentally, the NCW issue is information sharing – it is extremely difficult, if not impossible, for all the required parties to see and use each others' information due to fundamental incompatibilities that the support methodologies introduce into the information

technology systems. This section of the paper will examine several examples where systems and/or support methods inhibit rather than empower NCW.

Tasker Management. Tasker management is an excellent example to comprehensively exhibit how the current IT methods inhibit NCW. The "tasker" is a documented requirement for some kind of work. Tasker systems are used throughout the DoD. Normally, DoD staff elements use taskers for staff actions and not direct command and control of forces. As such, tasker information is sometimes associated with the non-military elements of national power – an important consideration as NCW at the combatant command level must consider and help synchronize all elements of national power.

Taskers drive much of the work that occurs at combatant commands – and the tasker management systems contain much of the information that this work generates. There is a diversity of tasker management systems in use in the combatant commands, as well as the Joint Staff. This diversity has lead to inaccessible information both inside and outside the commands, as well as ad-hoc methods to bridge the systems so that taskers can flow between the Joint Staff and the combatant commands, and between the combatant commands and their component commands. In some cases, this information, when stored in the personal account(s) of a staff member, is destroyed when that staff member departs a command. The impact on NCW is that much of the information generated by the work of combatant commands is excluded from present and future NCW shared awareness efforts, impeding progression to the self-synchronization sought through NCW methods.

For many years, EUCOM has used Microsoft Outlook as the IT software system supporting its tasker management business process. Using this system, little data is accessible beyond the action officer, except for those recipients of the emails generated by the business process. When action officers depart the command, IT management personnel delete their accounts for security reasons – along with all of the information they acquired and generated during their assignments.[27] Personal Outlook files are not publically searchable – so the user can only manually transfer this information by emails and attachments.

As a self-supporting IT services organization, EUCOM developed its own tasker management system. Several years ago, Outlook was a convenient tool that met the business process – NCW was not a factor and the extremely limited information availability was an acceptable risk. For several years, EUCOM has attempted, on its own, to develop, purchase, and implement other software systems to better support tasker management. To date, these efforts have been unsuccessful due to lack of resources in the Command, most notably government IT persons with business software expertise. The resulting deleterious second order effects of software customization to meet business processes and user training and acceptance have caused Outlook to remain in place, despite its information management and NCW issues.

EUCOM's components all use different tasker management systems. Of note, U.S. Air Force Europe (USAFE) has implemented a specifically tailored Microsoft product for tasker management that provides for information availability to all its users. Africa Command (AFRICOM), derived from and collocated with EUCOM, has chosen to

implement this same Microsoft product, tailored to the requirements of AFRICOM. EUCOM has chosen to replace its Outlook-based tasker management system with a government-owned software product originally designed for configuration management. This software has a user interface customized by EUCOM (using a contractor) for tasker management. While all these example commands have taken steps in a positive direction for information management and NCW, none of the tasker management systems are directly compatible, and will require "gluing together" of their respective data-management systems to create the information compatibility required for NCW.

The lack of a single common tasker management system across the DoD, or at least a set of compatible systems across the Joint community, is directly the result of the fractured methods used to deliver desktop IT services. DoD leaves each command to develop its own system – and each does so because it must. The combatant commands might realize a huge savings in staff effort if they had easy and routine access to all their previous work. Yet past work is often inaccessible at best. The "knowledge" foundation required to support shared awareness across the broad spectrum of combatant command work documented by taskers simply does not yet exist – and may not exist until an agency with the right expertise in information management, business enterprise software, and NCW develops and fields a common tasker management system across the Joint community.

TSCMIS. Several of the combatant commands have each developed their own Theater Security Cooperation Management Information Systems (TSCMIS). Each TSCMIS serves as an information focus point for the command's theater security cooperation programs, as well a tool to enhance the command's theater awareness

directly supporting command and control. The systems are the combatant commands' major IT link to information supporting the non-military elements of national power. The information contained in these systems is already essential to the shared awareness required by NCW. However, the lack of a single IT services provider for all the combatant commands has caused those who need a TSCMIS system to develop their own. There has been effort at the OSD level to pull the individual combatant commands' TSCMIS development processes together. While a good idea, this has created a competition between the commands for who's system will "win," requiring additional resources to be spent advertising and defending the existing systems. Without any single agency in place to both guide the development and become the program manager (PM), a single TSCMIS solution for all the combatant commands seems unlikely. The resulting system incompatibilities will continue to be an impediment to the seamless information sharing that NCW requires.

DMS. The Defense Messaging System (DMS) is an IT system that directly supports DoD-wide command and control (C2). DMS is essential to the combatant command C2 mission. All DMS messages are stored and thus form an historical record of combatant command C2 actions. This information is essential for the shared awareness required by NCW. Unlike standard email messaging, DMS has required delivery times, assured delivery, precedence, as well as security and directory service features tailored to the DoD mission. DISA has overall responsibility for the DMS, but the executive agents usually provide DMS service to the combatant commands. Each Service executes this mission differently, using different user software, and sometimes with indifferent funding priorities. The result is the combatant commands have different

user interfaces and different access to the stored messages. More importantly, the combatant commands sometimes find themselves embroiled in funding disputes with their executive agents over the continued financing of this vital system. When this enormous store of historical C2 data is transformed per DoD Directive 8320.02 to enable NCW data sharing, Service implementation and funding differences will likely not produce the unified results needed by the combatant commands for future NCW development. DMS also has an uncertain future, as DoD has not developed a replacement for this legacy system. If the DoD eliminates DMS without fielding an equivalent replacement, this could force the combatant commands to come up with their own individual solutions. The data and functional incompatibilities this could introduce would be detrimental to future DoD NCW efforts.

GCCS-J. The Global Command and Control System – Joint (GCCS-J) is the DoD Joint Command and Control (C2) enterprise information technology system of record tied most closely with implementing a user interface for NCW at the combatant commands. The DoD uses GCCS-J to correlate and share situational awareness and to monitor, direct, and execute missions. GCCS-J provides operational environment awareness by generating a near real-time picture necessary to conduct joint and multinational operations. The system integrates imagery, intelligence, status of forces, and planning information.[28] DoD fielded the GCCS-J to the combatant commands several years ago, and is currently developing and fielding periodic hardware and software upgrades.

There are several issues associated with local IT support and GCCS-J, a DISA program of record. Maintaining currency in hardware and software; and promoting

wide-spread use by combatant command personnel are the two most important issues affecting NCW capabilities. Each combatant command has responsibility for funding most GCCS-J upgrades (with funding from its executive agent); the PM then supports the purchasing, fielding, and training of GCCS-J upgrades in cooperation with the combatant commands desktop IT support process. As funding is almost always in short supply, GCCS-J funding requires prioritized recognition by the combatant commander. GCCS-J is not widely used outside of joint commands; therefore many senior commanders have only cursory knowledge of its capabilities. This makes it difficult for the IT staffs to get GCCS-J upgrades prioritized to achieve reliable and timely funding.

The lack of comfort with GCCS-J on the part of joint senior leadership as well as their staffs has led to limited use of GCCS-J. People tend to use enterprise IT systems that their leadership uses; when leadership avoids or works around an enterprise system, so does the rest of the organization.[29] For GCCS-J, the small user-base means limited user-demand for new or expanded capabilities. The system becomes stove-piped. A single common combatant command IT services provider could better manage the funding and upgrades, as well as promote the use of GCCS-J and other future NCW systems at the user level. Those same users could provide valuable feedback to a single agency where that feedback would affect current and future systems. As it is, combatant command users provide feedback on all IT systems to their local IT services providers, who in most cases have little or no influence over the fielded.

MNIS. The Multi-National Information Systems (MNIS) is a DISA program that provides the Combined Enterprise Regional Information Exchange System (CENTRIXS) and other coalition networking capabilities. DISA globally links the individual combatant

command CENTRIXS networks; the combatant commands own and operate their local network elements in virtually the same model as used for NIPRNet and SIPRNet capabilities. However, the CENTRIXS set of hardware and software is relatively limited and standardized so in theory, the data issues for NCW are far fewer than in the U.S.-only IT services discussed above. However, the tenuous year-to-year funding of the combatant command CENTRIX networks combined with the different forms of desktop IT support have created a static technology and user training situation. This effectively prevents any network(s)-wide improvements in NCW capabilities, such as the data sharing technique required by the DoD Directive "Data Sharing in a Net-Centric Department of Defense." [30]

Senior Leader Decisions. Combatant commands, in particular the geographic combatant commands, tend to be current operations-focused and have tightly constrained resources. Therefore, senior leadership decisions that impact desktop IT support within these commands will almost always give priority to the current operations requirements over long-term requirements such as implementing NCW-capable systems. Users generally view desktop IT support as a utility, much like electric power and telephone service. This could be a suitable model if IT support was regulated and provisioned like other utilities – regulated by DoD to international standards and provisioned by large, independent providers such as the Services and/or DISA. However, desktop IT support at the combatant commands is neither regulated (with the exception of security) nor independently provisioned. In all dimensions, with some security exceptions, it responds to the requirements of the combatant command. The combatant commands' focus on current operations, most especially in the geographic

combatant commands, makes it extremely difficult for them to support long-term NCW-enabling efforts.

Possible Solutions and Analysis

The solution space for supporting NCW through combatant commands' desktop IT support is fairly well constrained. A consistent constraint is the level of classification - Secret – and therefore the requirement for heavy involvement of U.S. government personnel and U.S. security clearances for most IT support personnel. The current desktop IT support solution is a diverse, evolutionary set of different support structures. It represents the least centralized, most locally-controlled overall solution. The most centralized solution would be for a single DoD Agency, most logically DISA, to provide centrally-managed desktop IT support for all the combatant commands. In the middle of this solution space would be the different IT support structures presently in place, with additional oversight and program management from JTF-GNO and DISA. These three points in the solution space are analyzed in detail below, with a focus on meeting the need to support NCW through desktop IT support at the combatant commands.

There are three major areas to examine when comparing and contrasting these three possible solutions. The first is the most critical – does the solution continue to support ongoing combatant command operations at least as well as the present solution? The second: does the solution significantly improve the future NCW capabilities of the supported command, inclusive of the JIIM environment, and the DoD? Finally, what resources and bureaucratic changes will the DoD have to make to implement the solution?

The status quo has managed to provide suitable desktop IT support to conduct current operations. As discussed previously in this paper, the status quo does not support NCW in a suitable manner, failing most particularly in the management of data and information, and the adoption of NCW-focused systems. In fact, it places the future of NCW in the combatant commands in peril. For that reason alone, it is not a suitable solution for the future of desktop IT support at the combatant commands. However, the current set of IT solutions does provide some significant advantages to some of the combatant commands, i.e. local control of both IT resources and the funding that buys and supports those IT resources. As this solution is also the current solution, changes to resourcing or bureaucratic systems are not required.

A solution that increases the oversight of DISA and JTF-GNO to control the separate combatant command desktop IT support systems could significantly improve the future of NCW in the combatant commands. This solution builds on the DoD IT support model already in place, in which JTF-GNO provides a significant level of network control focused on security, and DISA provides program management of a few DoD IT systems-of-record (e.g. GCCS-J and MNIS), some web-based DoD-wide NCW–enabling collaboration tools, as well as support and assistance with network security systems. This solution could improve the future of NCW IT systems within the combatant commands if it is able to overcome the significant resistance to “new and improved” that IT users exhibit when asked to give up their “tried and true” solutions. The major obstacles are choice and often the overwhelming current operations focus of some of the commands. The local IT support ownership of some of the combatant commands gives them an option; if they do not like the DISA-provided solution, they can

keep or seek their own. Stovepipe solutions do not support NCW within DoD or in the JIIM environment. Those commands with Service-provisioned solutions face the opposition of the Services to adapt their Service-oriented IT systems to include what are typically Joint-only solutions. Adaptation almost always costs resources. This solution does take advantage of existing resource and bureaucratic systems. However, it would require additional resourcing of JTF-GNO, DISA, and the combatant commands' IT services. Tighter control and additional PM work automatically incurs additional resource costs, with no offsetting savings. In addition, compliance with additional control and additional PM fieldings will require additional work by the IT support services at the combatant commands, again with no offsetting savings.

Handing over responsibility for all combatant command desktop IT support to DISA is not as radical a solution as might first appear. Presently, DISA provides DISN services to each of the combatant commands. Each combatant command has a supporting DISA field office. In terms of IT, the DISN brings high-capacity SIPRnet and NIPRnet connections from the Global Information Grid (GIG) to the combatant command desktop IT systems. DISA also provides some PM services, some web-based DoD-wide NCW–enabling collaboration tools (NCES) as well as a significant level of assistance via training, inspections, systems, and exercise support in the network security arena. Giving DISA responsibility for all elements of the combatant commands' IT support is the logical next step to strongly bolstering the future of NCW in the combatant commands and the DoD. It removes the most significant obstacle to IT systems that enable NCW at the combatant commands, mainly the reluctance and

inability of the combatant commands to pull their own resources away from the current operations mission to support future IT systems development and fielding.

An Example of Success

A DoD agency already successfully provides a service to all the combatant commands – and part of this successful service provisioning includes desktop IT support. The Defense Intelligence Agency (DIA) provides the Joint Worldwide Intelligence Communications System (JWICS) to each combatant command as part of an overall intelligence support package.[31] This IT support includes hardware, software, and DIA personnel and contractors to provide desktop support, plus future systems development, fielding, and training. DIA supports the combatant commands' intelligence IT completely, enabling the commands to focus their intelligence resources on their missions, rather than partially on intelligence IT support. This DIA JWICS support model, applied to collateral IT support, could strongly enhance NCW from a technology perspective. As a pure information services agency, DISA could bring much more expertise to the problem of improving desktop IT technology to support NCW than the one or two persons at each combatant command who might have this task as an additional duty; DISA could also bring more expertise to bear than any of the Services. A DISA solution follows the existing "chain-of-command" for NCW IT solutions. OSD/NII has the mission of enabling network-centric operations. The commander of DISA works for the Assistant Secretary of Defense, NII. DISA is already responsible within DoD for providing network-centric enterprise services – with the exception of the "last IT mile" to the desktops of the combatant commands. That "last IT mile" is absolutely critical to maximizing the NCW capabilities of the combatant commands.

Recommendations

1. DISA should prepare to assume responsibilities for desktop IT support to the combatant commands.

2. DISA should quickly assume support of the combatant commands' coalition desktop IT services as part of its MNIS program. The CENTRIX networks present an opportunity for DISA to assume a well-defined but small portion of desktop IT support duties for the combatant commands. As a test case, this should provide DISA and the DoD with the experience needed to eventually assume all combatant command desktop IT support.

3. DISA and combatant command representatives should study the DIA model used for providing intelligence support to the combatant commands. Where appropriate, DISA should analyze the experiences gained by DIA and adapt and adopt these experiences to support desktop IT support at the combatant commands. This study group must place special emphasis on supporting NCW.

4. DoD should extract the additional resources required by DISA from the existing desktop IT support structures at the combatant commands. This includes personnel and funding. DISA could adapt the Defense Working Capital Fund approach to include future costs of providing desktop IT support to the combatant commands, enabling baseline IT service costs to continue to be funded by the Services (as the combatant command executive agents), with optional and/or enhanced desktop IT support services to be funded by the requiring combatant command(s).

Conclusion

This paper has discussed desktop IT support at the combatant commands and its effect on NCW capabilities. With specific focus on information sharing as an enabler of the NCW tenet of self-synchronization, this paper examined several examples of current combatant command IT systems. It also examined the effects of combatant command senior leader decisions regarding IT support to current operations versus modernization to support DoD-wide NCW capabilities. The research revealed that the current desktop IT support methods do not adequately support combatant command NCW capabilities. After examining three possible future combatant command desktop IT support methods, this paper provided the recommendation, with supporting discussion, that DISA become the single provider of desktop IT support to all the combatant commands.

Endnotes

[1] David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, (The DoD Command and Control Research Program (CCRP) Publication Series, 1999), 35-36.

[2] David S. Alberts and Richard E. Hayes, *Understanding Command and Control*, (The DoD Command and Control Research Program (CCRP) Publication Series, 2006), 201.

[3] Michael G. Mullen, Capstone Concept for Joint Operations Version 3.0, (Washington, DC: U.S. Department of Defense, The Joint Staff, January 15, 2009), 4, 10, 33.

[4] U.S. Department of Defense, *Doctrine for the Armed Forces of the United States*, Joint Publication 1 (Washington, DC: U.S. Department of Defense, The Joint Staff J7, May 14, 2007), III-12.

[5] U.S. Department of Defense, *Functions of the Department of Defense and Its Major Components*, Directive 5100.01, (Washington, DC: U.S. Department of Defense, Assistant Secretary of Defense (Director of Administration and Management), August 1, 2002, Certified Current as of November 21, 2003), 3, 9-10.

[6] Donald Rumsfeld, Quadrennial Defense Review Report, (Washington, DC: The Department of Defense, February 6, 2006), 58-61.

[7] Alberts and Hayes, *Understanding Command and Control*, 2.

[8] Alberts, Garstka, and Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 114.

[9] *Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer*, "Vision/Mission," http://www.defenselink.mil/cio-nii/docs/card.pdf (accessed January 11, 2009).

[10] DISA Direct Home Page, "Defense Working Capital Fund (DWCF) Telecommunications Services Billing Prices for FY 2009," https://www.disadirect.disa.mil/products/asp/BillingRates/Final_DWCF_FY09_Price_Book_Ver11.pdf (accessed January 11, 2009), 3-31.

[11] U.S. Department of Defense, *Doctrine for the Armed Forces of the United States*, Joint Publication 1, III-14.

[12] U.S. Strategic Command, "U.S. Strategic Command Snapshot," http://www.stratcom.mil/fact_sheets/SnapShot.doc (accessed January 14, 2009).

[13] U.S. Strategic Command, "U.S. Strategic Command Snapshot," http://www.stratcom.mil/fact_sheets/fact_jtf_gno.html (accessed January 15, 2009).

[14] U.S. Department of Defense, *Doctrine for the Armed Forces of the United States*, Joint Publication 1, III-2 – III-3.

[15] For example, EUCOM Directive 50-1 defines the relationship between U.S. Army Europe – as the supporting "executive agent" – and EUCOM. ED 50-1 predates desktop computing, but does address communications support in the form of telephones and messaging.

[16] Two of the most pertinent directives are *Management of DoD Information Resources and Information Technology*, Directive 8000.01 and *Information Technology Portfolio Management*, Directive 8115.01.

[17] U.S. Department of Defense, *Management of DoD Information Resources and Information Technology*, Directive 8000.01 (Washington, DC: U.S. Department of Defense, Assistant Secretary of Defense (Networks and Information Integration), February 27, 2002, Certified Current as of April 23, 2007), 3.

[18] U.S. Department of Defense, *Information Technology Portfolio Management*, Directive 8115.01, (Washington, DC: U.S. Department of Defense, Assistant Secretary of Defense (Networks and Information Integration), October 10, 2005), 2-3.

[19] U.S. Department of Defense, *Data Sharing in a Net-Centric Department of Defense*, Directive 8320.02 (Washington, DC: U.S. Department of Defense, Assistant Secretary of Defense (Networks and Information Integration)/Department of Defense Chief Information Officer, December 2, 2004, Certified Current as of April 23, 2007), 2-3.

[20] U.S. Department of Defense, *Guidance for Implementing Net-Centric Data Sharing*, Guidance 8320.02-G (Washington, DC: U.S. Department of Defense, Assistant Secretary of

Defense (Networks and Information Integration)/Department of Defense Chief Information Officer, April 12, 2006), 11-15.

[21] U.S. Department of Defense, *Unique Identification (UID) Standards for a Net-Centric Department of Defense*, Directive 8320.03 (Washington, DC: U.S. Department of Defense, Under Secretary of Defense for Acquisition, Technology, and Logistics/Under Secretary of Defense for Personnel and Readiness, March 23, 2007), 5.

[22] The Joint Chiefs of Staff, *Joint Communications Systems*, Joint Pub 6-0 (Washington, DC: U.S. Department of Defense, The Joint Staff J6, March 20, 2006), III-4.

[23] Program Executive Office - Enterprise Information Systems, "Navy Marine Corps Intranet (NMCI)," https://enterprise.spawar.navy.mil/cmt_uploads/28/NMCI%20BLII-ONEnet.pdf (accessed January 12, 2009).

[24] U.S. Government Accountability Office, *Information Technology: DOD Needs to Ensure That Navy Marine Corps Intranet Program Is Meeting Goals and Satisfying Customers*, (Washington, DC: U.S. Government Accountability Office, December 2006), 2-5.

[25] Cynthia Rettig, "The Trouble with Enterprise Software," *MIT Sloan Management Review* 49, no. 1, (Fall 2007): 21-22.

[26] U.S. General Services Administration Millennia web page, http://www.gsa.gov/millennia (accessed January 12, 2009).

[27] With the exception of information the users placed in group-accessible network storage; this is not normally part of the tasker management business process and the data is not meta-tagged. A discussion of the structure and management of group-accessible network storage is an important part of information sharing and thus NCW, but beyond the scope of this paper.

[28] U.S. Department of Defense,"Defense Information Systems Agency Global Command and Control System – Joint ," http://www.disa.mil/gccs-j/, (accessed January 12, 2009).

[29] John E. Ettlie et al., "Strategic predictors of successful enterprise system deployment," *International Journal of Operations & Production Management* 25, no. 10, (2005): 956.

[30] U.S. Department of Defense, *Data Sharing in a Net-Centric Department of Defense*, Directive 8320.02, 2-3.

[31] Sharon A. Houy, "Working Together: Why DIA Now Employs Combatant Command Intel Agents," *Armed Forces Journal*, (December 2008): 34, 37.

DEPARTMENT OF THE ARMY
UNITED STATES ARMY WAR COLLEGE AND CARLISLE BARRACKS
CARLISLE, PENNSYLVANIA 170135050

December 16, 2009

REPLY TO
ATTENTION OF

ATWC-AA

Defense Technical Information Center
Mr. Lawrence Downing
Information Security Officer
ATTN: DTIC-OQ
8725 John J. Kingman Road
Fort Belvoir, Virginia 22060

Dear Mr. Downing:

Colonel David A. Barlow has requested a change in the Distribution Availability Statement associated with his 2009 United States Army War College Strategy Research Project title: "Impending Network Centric Warfare: Combatant Command Information Technology Support," ADB349930. The original Distribution Availability Statement (Distribution B: authorized to U.S. Government Agencies only) was assigned in error as the document was intended for public release. This request was initiated by the author and carries the endorsement of both his Project Adviser, Dr. Jeffrey L. Groh and the Director of Communicative Arts.

Larry D. Miller, Ph.D. M.S.S.
Director, Communicative Arts
(717) 245-3358
Larry.D.Miller@us.army.mil