REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*
(23-10-2006)

2. REPORT TYPE
FINAL

3. DATES COVERED *(From - To)*

4. TITLE AND SUBTITLE
The BORG: Network Centric Operations

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

COL Michelle M. Fraley

Paper Advisor (if Any):

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

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

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

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

10. SPONSOR/MONITOR'S ACRONYM(S)

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

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

The National Defense Strategy lists eight desired capabilities and attributes of our joint force. Conducting Network Centric Operations (NCO) is one of the eight capabilities providing the Department of Defense transformation focus. Despite academic guidance from the Information Superiority Metrics Working Group (ISMWG), and published goals and objectives from the Joint Staff, a key player remains in the background- the Geographic Combatant Commander (CCDR). As a result of the Unified Command Plans 2002 thru 2006, there have been several organizational changes which include the Commander, DISA, as JTF-GNO under USSTRATCOM, to lead the Department of Defense to a Net-Centric Environment. This paper defines the components of NCO, but concentrates on three dimensions in the information domain to show, using six cases, that the CCDR is needed with DISA's regional Theater Network Center (TNC) as part of the Geographic Combatant Command's (GCC's) team to operationalize NCO. The paper draws a conclusion that the CCDRs are the players who can develop a joint professional net-centric force, by influencing the future of Service Component platforms (physical domain), but most importantly providing the network-value leadership to shape the information domain. Finally, the paper recommends changes to the current NetOps structure to make the TNC the execution arm of the CCDR for net-centric operations.

15. SUBJECT TERMS

value network leadership; high value networks; customer intimacy strategy; Theater Network Center (TNC); Theater NetOps Control Center (TNCC); Joint Communications System Campaign Plan; JTF-GNO

16. SECURITY CLASSIFICATION OF: UNCLASSIFIED			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Chairman, JMO Dept
a. REPORT UNCLASSIFIED	**b. ABSTRACT** UNCLASSIFIED	**c. THIS PAGE** UNCLASSIFIED		31	**19b. TELEPHONE NUMBER** *(include area code)* 401-841-3556

NAVAL WAR COLLEGE
Newport, R.I.

THE BORG: Network Centric Operations

by

Michelle M. Fraley

COL, United States Army

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: ______________________

23 October 2006

Abstract

THE BORG: Network Centric Operations

The National Defense Strategy lists eight desired capabilities and attributes of our joint force. Conducting Network Centric Operations (NCO) is one of the eight capabilities providing the Department of Defense transformation focus. Despite academic guidance from the Information Superiority Metrics Working Group (ISMWG), and published goals and objectives from the Joint Staff, a key player remains in the background- the Geographic Combatant Commander (CCDR). As a result of the Unified Command Plans 2002 thru 2006, there have been several organizational changes which include the Commander, DISA, as JTF-GNO under USSTRATCOM, to lead the Department of Defense to a Net-Centric Environment. This paper defines the components of NCO, but concentrates on three dimensions in the information domain to show, using six cases, that the CCDR is needed with DISA's regional Theater Network Center (TNC) as part of the Geographic Combatant Command's (GCC's) team to operationalize NCO. The paper draws a conclusion that the CCDRs are the players who can develop a joint professional net-centric force, by influencing the future of Service Component platforms (physical domain), but most importantly providing the network-value leadership to shape the information domain. Finally, the paper recommends changes to the current NetOps structure to make the TNC the execution arm of the CCDR for net-centric operations.

The Borg: Network Centric Operations
"Resistance is futile…"

Table of Contents

List of Illustrations

INTRODUCTION

To reach its full potential, Network Centric Operations (NCO) must be deeply rooted in operational art, utilizing military forces to achieve strategic, operational and tactical objectives by maximizing (emphasis mine) the physical, information and cognitive domains through the creative imagination of the Geographic Combatant Commander (CCDR).[1] The Department of Defense (DoD) defines NCO as a concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed on command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization.[2] NCO involves the interaction of the physical, information and cognitive domains to create value (combat power) from information.[3] The CCDRs play a vital role toward the operationalization of NCO by becoming the value-network leadership, and taking reigns of the tacit knowledge core of the DoD value network-the Global Information Grid (GIG).[4] Value network leadership is defined as the active management of technical knowledge, data that is stored and transferred easily within and among Services, to tacit knowledge, information that arises from joint experience of the people in the Services.[5] An analogy in achieving a net-centric operational environment is the Borg Collective in the movie Star Trek First Contact, where the Collective (Geographic Combatant Command (GCC)/Joint Task Force (JTF)) makes decisions as a single entity; however, the Borg Queen (CCDR/JTF CDR) plays a leadership role in ordering the chaos of the Collective and the information flowing in from its millions of drones (soldiers, marines, sailors and airmen).[6] Because the GCC can not assimilate its Component Service commands, the CCDR must approach the Service Components "to partner in value networks as an integrated collaboration of specialist companies, each providing complementary intermediate services."[7] Assimilation of Component Service commands, as symbolized in Star Trek First Contact with the various cybernetic implants and hardware, would strip the Components of their individuality, and the GCC would lose the specialized contribution of that Service Component. The challenge at hand is how to balance requirements of net-centricity against the Services' tacit (information domain) and technical (physical domain) knowledge assets.[8] The thesis is that the CCDRs are in a better position than the Joint Staff and Service Chiefs to capture, define, and mature that balance. The DoD can not attain joint network centricity without the CCDRs providing value-network leadership to create the superadditivity of the physical, information, and cognitive domains-maximizing (emphasis mine). Figure 1 (The Borg: Network-Centric Operations) conceptually depicts the superadditivity of the physical (Service platforms), information and cognitive domains and the maximizing (emphasis mine) effect that can be attained through the value network leadership of the CCDR. Each GCC has a unique mix of forces from the Services based on the requirements of his geographic region which dictates how the network value leadership realizes a customer-intimacy strategy. The value network possesses capabilities that precisely match a Service's requirements, but others (GCC, other Services and Agencies, Coalitions, and Intergovernmental/Nongovernmental Organizations (IGO/NGOs)) have the ability to extract services that have a high return. These services cover as a minimum the operational functions of command and control, intelligence, maneuver, logistics, fires, and protection. Figure 2 (The Issue: Network-Centric Operations) depicts conceptually the current status where the CCDR gets no better maximizing (emphasis mine) effect than a Service's tacit (information domain) and technical (physical domain) knowledge.

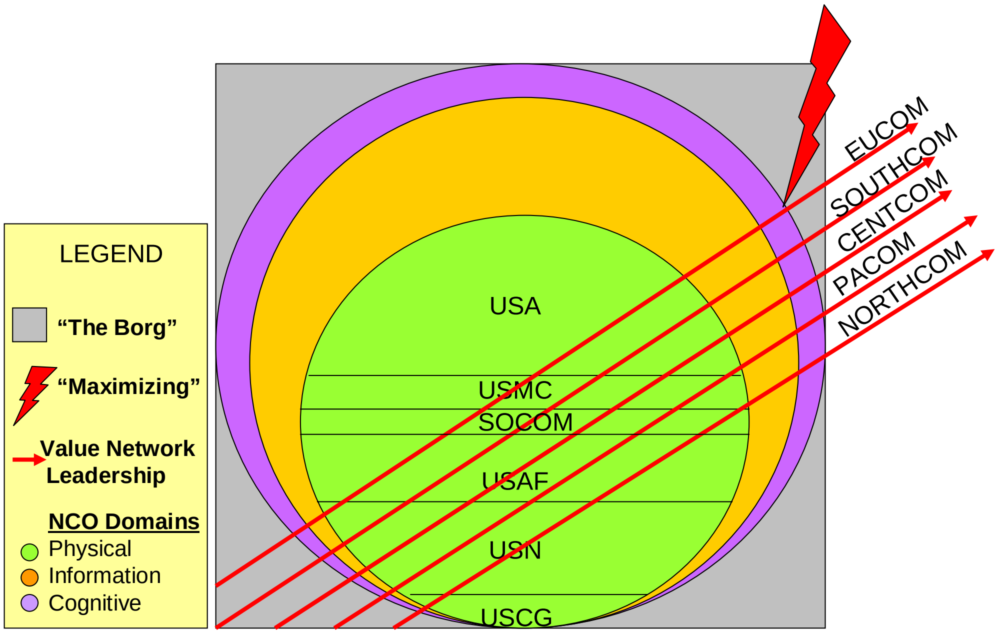


Figure 1. The Borg: Network-Centric Operations

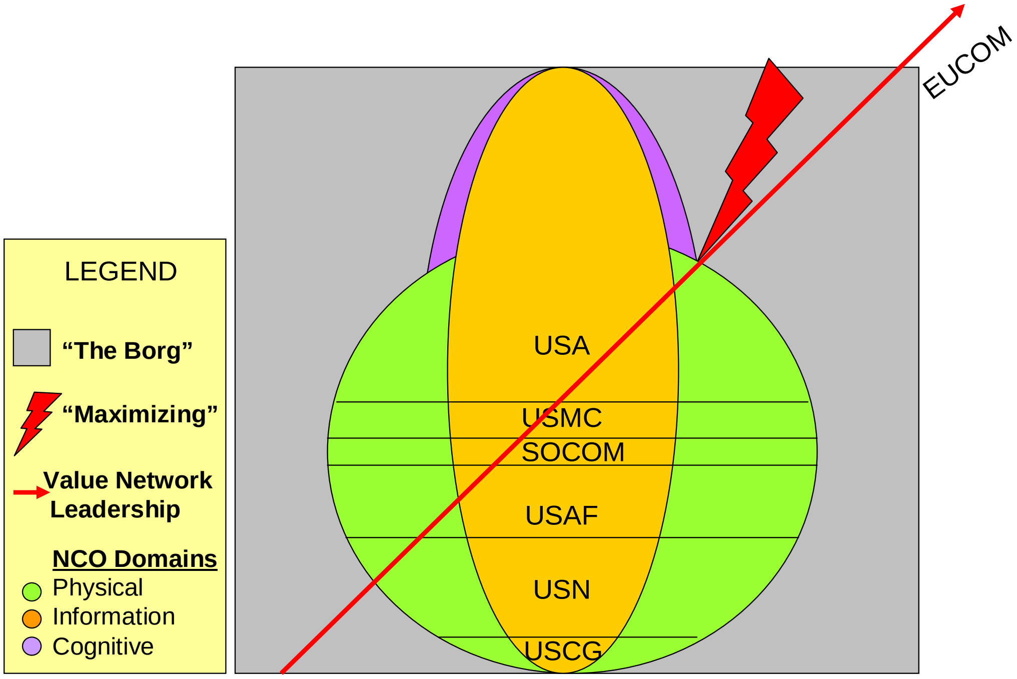


Figure 2. The Issue: Network-Centric Operations

BACKGROUND

The National Defense and the National Military Strategies identify the conditions of NCO as ends (emphasis mine) -"We will conduct network-centric operations with compatible information and communications systems, usable data, and flexible operational constructs."[9] However, the means (emphasis mine), and ways (emphasis mine) are left unanswered; what actions will produce the condition of NCO (ways), and how will joint and Service Component resources be applied to accomplish the actions (means) to attain the conditions of NCO (ends)?[10] The CCDRs provide the conceptual linkage of ends, ways, and means through their campaign plans (ways) leveraging Service Components (e.g. Army, Navy, Air Force), joint and functional (e.g. TRANSCOM, STRATCOM, SOCOM) resources (means). The Joint Chiefs of Staff (JCS) and the Office of the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer have published concept documents such as the Joint Communications Systems Campaign Plan, and the Net-Centric Checklist Version 2.1, to identify goals and objectives for the next two to five years, and "assist program managers in understanding net-centric attributes required for programs to move into the net-centric environment in the GIG."[11] The proposition is that the CCDRs are in a better position than the Joint Staff and Service Chiefs to capture, define, and mature net-centricity through the clear understanding, active management, and Service-intimacy balance of the three NCO components-the physical, information, and cognitive domains.[12] Insertion of new technology without organizational or procedural (Tactics, Techniques and Procedures (TTPs)) changes is "picking low-hanging fruit."[13] This is exemplified with the Army's Stryker Brigade Combat Team (SBCT).[14] The Service platforms and associated connecting networks are the physical domain.[15] In the

SBCT, the platform consists of the Stryker vehicle family, the SBCT digital communications network, and the Army Battle Command Systems (ABCS).[16] "The information domain is where information is created, manipulated, and shared."[17] During OIF, the Force XXI Battle Command Brigade and Below Blue Force Tracking (FBCB2BFT) provided a view of friendly forces from seven different systems thru a gateway.[18] During the march on Baghdad, FBCB2BFT provided the Commander, 3rd Bn, 1st BCT visibility over 2nd BCT's change in route, followed by a phone call thru Joint STARS (Joint Surveillance Target Attack Radar Systems) to confirm enemy disposition.[19] LTG Boutelle explained, "The BFT-enabled platforms transmitted and received battle field locations, battlefield graphics and overlays, and orders to and from a central information server system for aggregation and retransmission."[20] The mind of the CCDR is the cognitive domain.[21] Using the SBCT platform and the tacit knowledge from FBCB2BFT, the cognitive domain of the 3rd Battalion Commander immediately triggered a change of mission to a hasty defense versus his original mission bridgehead defense.[22] As stated by the battalion commander, "Moving from a bridgehead defense to a hasty defense turned out to be very, very important because there was an Iraqi counterattack and there were two companies on the far side of the bridge."[23]

Understanding the three NCO domains (physical, information, cognitive) to achieve the <u>ends</u> (emphasis mine), allows us to direct our attention to the resources <u>means</u> (emphasis mine) that the CCDR has available to achieve NCO. As a result of Unified Command Plan (UCP) 2002 thru 2006, and USSTRATCOM's new roles and responsibilities, the Commander, Defense Information Systems Agency (DISA) became the Commander, Joint Task Force-Global Network Operations (JTF-GNO) on 18 June 2004 to lead the DoD towards a Net-Centric warfighting future.[24] The DISA Commander, Lt Gen Croom reports directly to USSTRATCOM Commander, GEN Cartwright.[25] Within each GCC, the JTF-GNO operates through Theater Network Centers (TNCs); the TNCs provide technical support and execution TACON to the GCC.[26] The TNC is an O-6 centrally selected command position under DISA. This paper will specifically address how the CCDR can influence the information domain using the TNC as the execution arm. In the words of Vice Admiral Nancy Brown, the Joint Staff's Director for Command, Control, Communications and Computer Systems, "We don't have a very good joint training track in the concepts of net-centric operations. And we really haven't developed a professional force that can take us to the next level of employing the capabilities that a net-centric environment provides."[27] The CCDRs are the leaders who can develop a joint professional net-centric force, by shaping the future of Service Component platforms, but most importantly shaping the information domain through the regional TNCs and their portion of GIG. The CCDRs must embed the DISA-owned regional TNCs in the everyday battle rhythm of their respective J3s as the de facto Theater NetOps Control Center (TNCC); the command relationship between USSTRATCOM and DISA (JTF-GNO) must be replicated at the CCDR's level with the regional DISA commander (DISA-Europe, DISA-Pacific, etc.); and Theater Security Cooperation (TSC) activities, and training exercises must be used as proof of concept to net-centric operations tasks that become part of the CCDR's strategy map that support Department of Defense and Joint Staff driven ways, means and ends. Figure 3 depicts JTF-GNO's relationship to USSTRATCOM.[28] Figure 4 describes the GCC's TACON relationship to the TNC.[29] The TACON relationship is limited to the detailed direction and control in the application of assets to accomplish missions or tasks assigned.[30] The TNCC which belongs to the GCC receives direct support from the TNC which works for regional DISA Commander.[31]

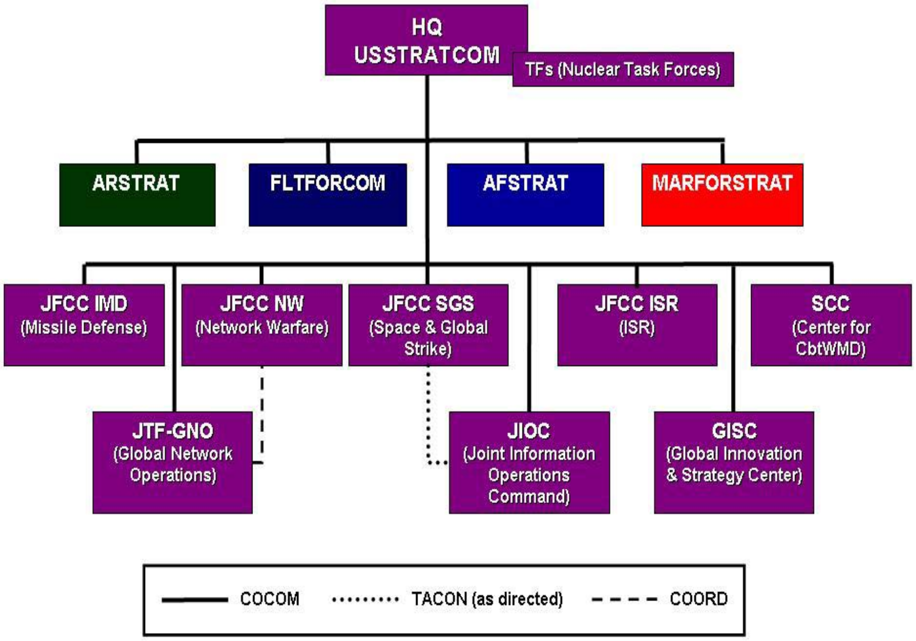

HQ
USSTRATCOM
TFs (Nuclear Task Forces)
ARSTRAT
FLTFORCOM
AFSTRAT
MARFORSTRAT
JFCC IMD (Missile Defense)
JFCC NW (Network Warfare)
JFCC SGS (Space & Global Strike)
JFCC ISR (ISR)
SCC (Center for CbtWMD)
JTF-GNO (Global Network Operations)
JIOC (Joint Information Operations Command)
GISC (Global Innovation & Strategy Center)
COCOM
TACON (as directed)
COORD

Figure 3. USSTRATCOM Organization

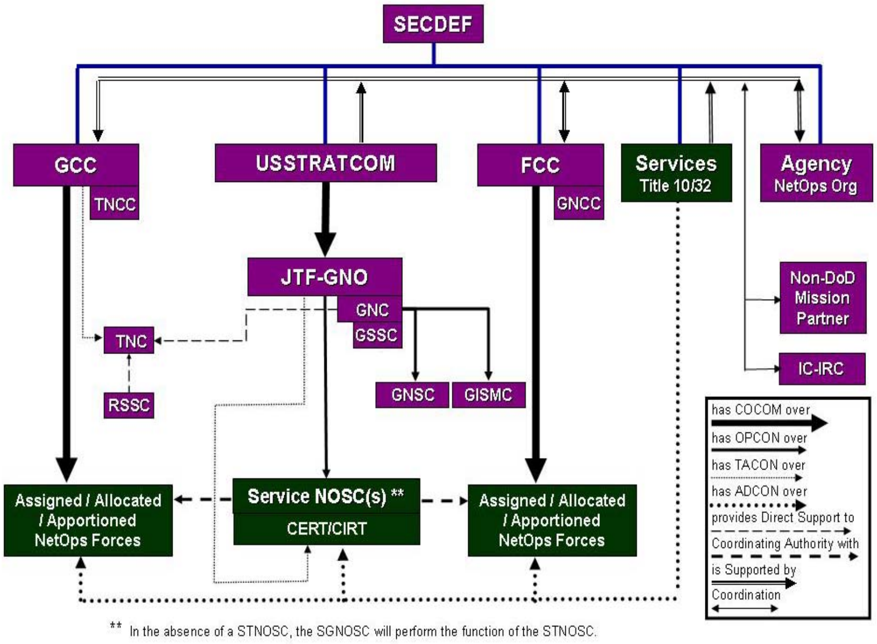


Figure 4. Global NetOps C2

DISCUSSION and ANALYSIS

The methodology to do the analysis and defend the thesis- The CCDRs are the leaders who can develop a joint professional net-centric force, by shaping the future of Service Component platforms, but most importantly shaping the information domain using the TNC as the execution arm. - will use the ground rules already established by the Information Superiority Metrics Working Group (ISMWG) sponsored by the Command and Control Research Program (CCRP), and the goals and objectives published in the Joint Communications System Campaign Plan by the JCS J6. These two entities have respectively established academic and conceptual strategic templates that need the value network leadership of the CCDRs to be operationalized. Academically, the ISMWG has defined the three major dimensions of the information domain as richness (emphasis mine)/quality of the information domain, reach (emphasis mine)/distribution of the information domain, and the quality of interaction (emphasis mine) within the information domain.[32] The attributes of completeness, timeliness, and relevance will be addressed in richness.[33] In the dimension of reach, we will discuss geographic range, sharing across alliance/coalition organizations, and latency.[34] Data, voice, and video information exchange will be considered in the dimension of interaction.[35] The academic template framing the information domain, will be cross-walked versus approved goals and selected objectives in the Joint Communications System Campaign Plan which include six Network Centric Environment (NCE) operating capabilities (Knowledge Management, Information Assurance, Network Management, Information Transport, Enterprise Services, and Applications).[36] The six JCS approved goals are the following: Goal 1- Connect the Warfighter; Goal 2- Leverage the Power of the Enterprise Services; Goal 3- Secure the Network; Goal 4- Accelerate Information Sharing;

Goal 5- Synchronize Delivery of Network Capabilities; and Goal 6- Transform GIG Enterprise Management and Enhance Electromagnetic Spectrum Access.[37] It is noteworthy to highlight that only two of 202 actions under the six Goals and thirty-five objectives have been assigned (designated as Office of Primary Responsibility-OPR) specifically to the GCCs; however, thirty-three actions have been assigned to DISA or USSTRATCOM/JTF-GNO, and five actions to the Services. The distribution of the 202 actions is a reflection of the lack of leadership and focus at the theater strategic level, which contributes to the perception that NCO will result in the commander at the operational level becoming a spectator, and not an actor in both the information and cognitive domain of NCO. Figure 5 is a notional depiction of the CCDRs' contribution to NCO. In the 20th Century, the CCDR was at the mercy of a platform-based environment (stovepipe); the perception in 2006 is that the CCDR has little to no contribution to net-centricity. However, net-centricity in support of Vision 2020 requires full spectrum dominance focused on operational forces.

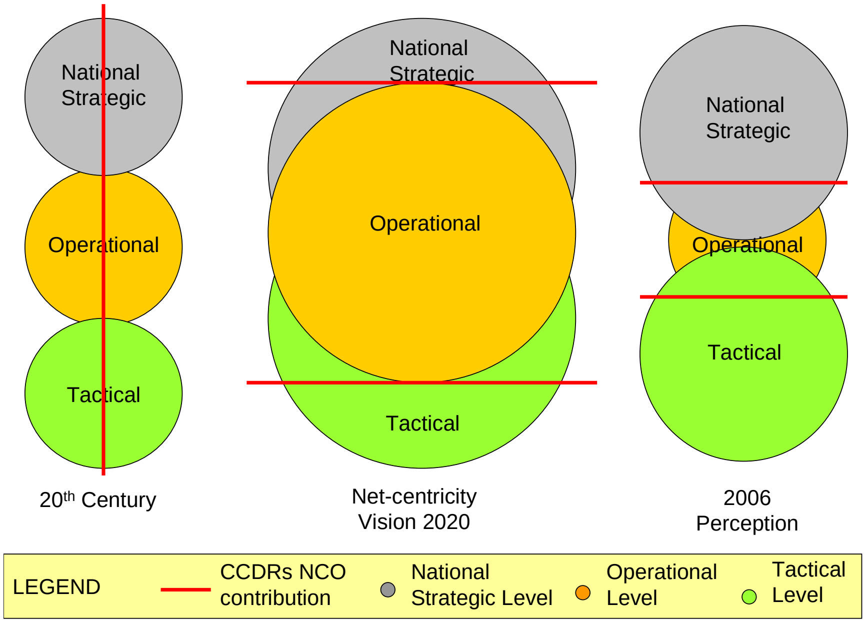


Figure 5. CCDR's contribution to NCO

Figure 6 depicts a non-inclusive cross-walk that will be used in support of the discussion and analysis. For the purposes of this paper, six cases will be used to demonstrate how the GCC can use the regional TNC (DISA) to shape the information domain and provide the value network leadership needed to attain NCO. The specific objectives extracted from the Joint Communications System Campaign Plan that will be addressed have been color coded in green in Figure 6. The objectives are the following:

Objective 1.2: Orchestrate Collection, Validation, and Implementation of Joint Warfighting Capabilities into Existing Information infrastructure and the Defense Information Systems Network (DISN);

Objective 2.2: Establish and Advocate Net-Centric Enterprise Service Capabilities Required to Support DoD Joint Net-Centric Operations (JNO);

Objective 3.5: Establish Methods and Measures of Effectiveness to Identify and Periodically Assess DoD Ability to Secure the Network;

Objective 4.4: Improve Multi-National Information Sharing (MNIS) Capability by Sustaining Current Operational Systems, Transitioning to Enterprise Architecture, and Supporting the Development of Objective Information Sharing Capability;

Objective 5.4: Define Common Communications System Modeling and Simulation (M&S) Tools that Support Joint Communications System Planning and Execution

Objective 6.1: Develop Policy and Governance Structure to Facilitate End to End (E2E) Enterprise Management

Joint Staff J6 Goals and Objectives ISMWG Information Domain dimensions and attributes	Goal 1: Connect the Warfighter	Goal 2: Leverage the Power of Enterprise Services	Goal 3: Secure the Network	Goal 4: Accelerate Information Sharing	Goal 5: Synchronize Delivery of Network Capabilities	Goal 6: Transform GIG Enterprise Management and Enhance Electromagnetic Spectrum Access
Richness: Quality of the information domain						
Completeness: Relevant entities/sets such as key parts of the enemy force, key weather and terrain		Objective 2.3				
Timeliness: Data is where it is needed, when it is needed	Objective 1.2			Objective 4.1		
Relevance: information necessary for success/crucial element to satisfy C4ISR systems	Objective 1.6	Objective 2.2				
Reach: Distribution of the information domain						
Geographic Range: Coverage of information sharing end to end	Objective 1.1	Objective 2.4			Objective 5.2	Objective 6.1
Sharing across alliance/coalition: Information crossing broader organizations	Objective 1.4		Objective 3.1	Objective 4.4	Objective 5.8	
Latency: Sharing information sooner not routed thru central processing location	Objective 1.3				Objective 5.4	
Interaction: Quality of interaction within the information domain						
Data: NIPR, SIPR, JWICS	Objective 1.5	Objective 2.1	Objective 3.5			
Voice: DSN, VoIP, DRSN		Objective 2.1	Objective 3.5			
Video: VTC, IWS, DCTS		Objective 2.1	Objective 3.5			

Figure 6. Information Domain and JCSCP Crosswalk

Case #1: Goal 1, Objective 1.2, Action 1.2.5: Assess requirements for redundant (backup) systems and diverse network routing (OPR: DISA-1QFY09); Information Domain dimension of richness with the attribute of timeliness.[38]

Discussion #1: The regional TNCs (DISA) are in a better position to evaluate redundancy and diversity within the GCCs AOR knowing employment of forces.   For example, knowing that the SBCT in Vilseck, GE conducts its everyday business from the Area Processing Center in Grafenwoehr, GE with redundant and diverse routing, and data failover capability in Kaiserslautern, GE provides the focus in analyzing the type of data that needs to be pushed during a deployment to meet the requirement of where and when it is needed. The CCDR can use the TNC to extend the existing network-centric conditions within the SBCT outside of sanctuary during a TSC exercise in Bulgaria simulating both an austere (extending the tactical mile with SATCOM to a Satellite Tactical Entry Point (STEP) site), or a more robust environment (using a commercial entry point from a DISA owned/leased point of presence). The focus in this case becomes crossing Microsoft Exchange domains (EUCOM and CENTCOM), or tunneling coalition data such as the Combined Enterprise Regional Information Exchange System (CENTRIX) without compromising security to meet the attribute of timeliness. This is an area of technical expertise within the regional TNCs that could become part of the training objectives during TSC exercises. There were lessons learned during deployment of Europe-based units whose data from sanctuary could not be made available in a timely manner during Reception, Staging, Onward Movement and Integration (RSOI), and once made available it was at the expense of millions of dollars of SATCOM bandwidth to replicate locally with days/week-old data.

Case #2: Goal 2, Objective 2.2, Action 2.2.4: Monitor and coordinate with DISA to ensure Defense Messaging System (DMS) is moved into a Network Centric Environment (NCE) and ensure it remains sustainable to support organizational messaging through 2012 (OPR: DISA-3QFY08); Information Domain dimension of richness with the attribute of relevance.[39] Discussion #2: The termination and replacement of the Automatic Digital Network (AUTODIN) with the Defense Messaging System (DMS) is still remembered by many of as the biggest emotional event in organizational messaging since the 1970's. Several commands who were used the old "read files" prepared by the Telecommunications Centers (TCCs) continue to wonder what to do with the hundreds of organizational messages coming thru DMS awaiting to be routed to someone's Non-secure Internet Protocol Router Network (NIPRNET) or Secure Internet Protocol Router Network (SIPRNET) account. DMS remains in many ways a <u>stovepipe</u> (emphasis mine) system operationally and technically known by few users and administrators. The regional TNCs have government employees, and in some instances contractors with a lot of experience on DMS, specifically the issues associated with its use or non-use at the GCC level. Some of the reluctance to use DMS stems from the number of irrelevant messages that are automatically forwarded to users. Organizational messaging is a necessary evil, but requires a lot of attention by the regional TNC to understand its operational impact in relationship to the business process of the GCC. Taking into account the cost of DMS software and hardware, interface equipment with the Automatic Messaging Handling System (AMHS), training of personnel, and accreditation to include NSA approved High Assurance Guards (HAG), the action that should be taken by the regional TNCs is how quickly to migrate from DMS to meet relevance of information for the CCDRs.

Case #3: Goal 3, Objective 3.5, Action 3.5.6: Incorporate and assess Information Assurance (IA) activities in all joint exercises; address shortfalls and determine process to track IA and Computer Network Defense (CND) events in joint exercises planning conferences and after action reports (OPR: USTRATCOM (JTF-GNO)-1QFY07); Information Domain dimension of interaction with the attribute of data, voice and video.[40]

Discussion #3: IA and CND events down to the desktop account for a large percentage of incidents; therefore, the CCDRs and associated TNCs are in a better posture to address the realities associated with Service/coalition enclaves, local area networks, and desktop Information Assurance Vulnerability Alert (IAVA) compliance. As Service Component enclaves move towards an IP-based/Dynamic Host Configuration Protocol (DHCP) environment, the interaction between data, voice and video in the secure and non-secure modes will become more prevalent in the form of collaborative tools. The discipline and acceptable behavior must have its roots at the CCDR level with data provided by the TNC to the J3 from the daily battle rhythm between the GCC, subordinate Service Components, DoD agencies, and others. IA and CND tracking must be done daily to provide a meaningful methodology and measure of effectiveness that can be applied during joint exercises, and extend to the multinational/coalition/interagency levels. There are already mature IA and CND activities within the GCCs AOR with the Service Components. Within the last year, DoD mandated actions such as password changes to thousands of routers and switches which did not complement previous DoD directed events. Patching and vulnerability scanning software such as Citadel HERCULES and eEye RETINA, not fully matured, are being fielded. There has to be a homogenous daily approach within a CCDR's enclave to IA and CND to eventually mature and extend that business process throughout the GIG.

Case #4: Goal 4, Objective 4.4, Action 4.4.9: Develop a globally reaching interactive fully functional information network (GRIFFIN) web and chat initial operational capability with the United States, United Kingdom, and Australia (OPR: DISA-1QFY07); Information Domain dimension of reach with the attribute of sharing across alliance/coalition.[41]

Discussion #4: Assuming that this globally reaching network will serve at the national strategic level (White House) down to the operational and tactical level in a multinational and interagency environment, it is imperative that both EUCOM and PACOM with their respective theater TNCs play a critical role from both an operational and sustainment perspective. Capabilities should be on par with what the US and the UK have already developed through Standard NATO Agreements (STANAG), and the CENTRIX in addition to anything that has been developed between PACOM and Australia through the myriad of exercises, and the Range of Military Operations (ROMO) such as Operation Stabilize in East Timor. The regional DISA TNCs could partner with the White House Communications Agency (WHCA), a subordinate command of DISA, to develop an interoperability capability that spans the spectrum of operations and serves not only the military but the diplomatic (President, Department of State), information (National Security Advisor), and economic (G8, UN) elements of national power. Exercises such as Combined Endeavor in Baumholder, GE could be easily expanded using the STEP sites and DISN core capabilities from DISA to connect the US, UK, and Australia national strategic levels, PACOMs operational level with the British EUROMUX (tactical communications), Australian equivalent, and US Joint Network Node (JNN)/Data Communications Packages (DCP). Additional complexities using the IRIDIUM MERCURY capability can be incorporated to test multi-level security issues.

Case #5: Goal 5, Objective 5.4, Action 5.4.3: Submit Network Warfare Simulation (NETWARS) communication device model standards for inclusion in the DoD Information Technology Standards Registry (DISR) (OPR: DISA-3QFY07); Information Domain dimension of reach with the attribute of latency.[42]

Discussion #5: The nature of Modeling and Simulations (S&M) presents a challenge in the Information Technology world and its dynamic environment. There are two features of modeling that must be well understood and defined in order to derive any utility from static S&M tools. The first feature, the form of a model, translates to the method of representation which could be mathematical (latency of data for example), verbal, or pictorial.[43] The second feature, the content of a model, is what you want to represent which could be connectivity, routing pattern, or time first data packet was sent, and the last data packet was received to complete transmission of a determined data unit.[44] There are enormous gaps between what is perceived that needs to be modeled at the theater strategic level versus that which needs to be modeled at the operational and tactical levels. The nature of Goal 5 requires that these gaps among modeling environments are addressed by the value network leadership of the CCDR with the technical expertise of the regional TNC; otherwise, S&M tools could produce a false representation of the reach dimension within the information domain. The number of TSC activities in each GCC provides a natural environment to experiment with S&M tools with defined training objectives that have the potential to frame S&M requirements. In our current environment, most of the S&M tools address the national and theater strategic environment which is very robust, and does not suffer from the myriad of shortfalls existing at the last tactical mile.

Case #6: Goal 6, Objective 6.1, Action 6.1.8: Formalize and establish NetOps Community of Interest (COI) directive and structure and complete Network Operations (NetOps) data strategy (OPR: USSTRATCOM-4QFY07); Information Domain dimension of reach with the attribute of geographic range.[45]

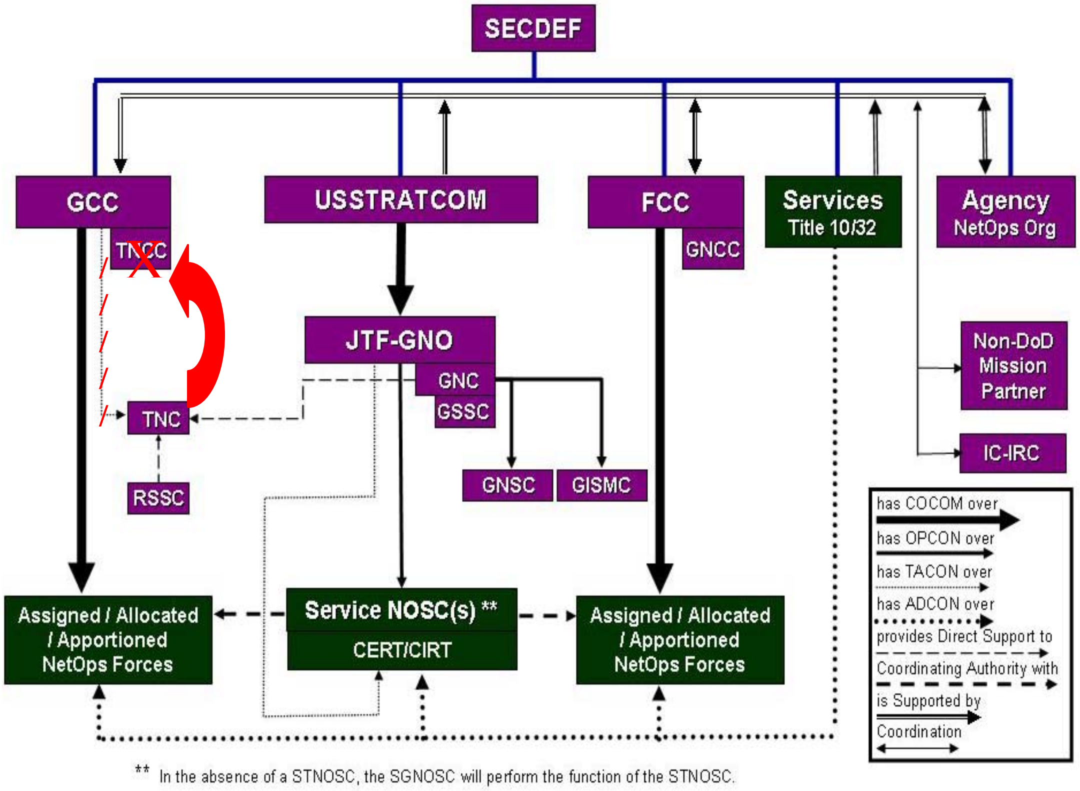
Discussion #6: The objective as defined by the Joint Staff is to move control and visibility of the GIG from its current Service-centric view toward a GCC-centric view.[46] This objective and specific action assigned to USSTRATCOM touches the very essence of this paper's thesis. Unlike other assigned objectives, the use of USSTRATCOM as OPR versus DISA or JTF-GNO makes you question our chain of command's understanding of the role that network value leadership has in the implementation of NCO. Unfortunately, USSTRATCOM has no credibility in the area of NetOps unless it uses the DISA/JTF-GNO as a front-end to reach this objective. The Joint Concept of Operations for Global Information Grid NetOps, published by JTF-GNO, does a very poor job identifying in generic terms the COI, which include in addition to the Department of Defense, multi-national, NGO, interagency, and IGO players. Additionally, command and control relationships are ill-defined, and in the case of the DISA-owned regional TNCs, the TACON command and control relationship to the GCC is not substantiated with on the ground command relationships and rating schemes. GCCs are standing up their own TNCC because they do not see the TNC as part of the organization. The result is two separate organizations (TNCC and TNC) in different facilities using similar tools, capabilities, and personnel skills simultaneously pursuing an OPCON relationship with the Service Theater NetOps and Security Center equivalents (STNOSC) with no value network leadership providing superadditivity to the physical, information, and cognitive domains of NCO.

CONCLUSIONS

As the analysis of the six cases previously discussed demonstrates, the CCDR must play a vital role to operationalize NCO. The CCDR provides the network value leadership to maximize (emphasis mine) the potential in the physical, information and cognitive domains to attain high-value networks. The CCDRs are the DoD's best option to achieve the desired end state that the Secretary of Defense has articulated in the National Defense Strategy from the national strategic down to the tactical level. The CCDRs can realize the customer value intimacy strategy where Service Component do not see themselves as competitors, but instead draw services from the value network precisely matching their Service requirements.[47] Operationalizing NCO results in the GIG become a high value network drawing its comparative advantage from the tacit knowledge that is jointly held by the Services.[48] There is a competitive advantage due to the idiosyncratic nature of the value network (GIG) that is derived from the richness, reach and interaction dimensions within the information domain.[49] The execution arm to net-centric operations within the GCC should be the regional DISA TNC. This organization which falls under DISA has the implied task to lead net-centricity as an extension of USSTRATCOM's JTF-GNO's charter; however, it must lead as part of the CCDRs authority in an AOR, and not as a staff organization. In a net-centric environment the Services are not independent partners, but part of a continuous and adaptive ecosystem that, as in the case of the Borg, has the ability to adapt nearly instantaneously to any type of attack or threat.[50] Focusing its resources on the threat at hand all possible outcomes and responses can be explored within an extremely short period of time to derive combat power. Additionally, actions associated with attaining net-centricity must be mapped to the GCC's ways, means, and ends as a bridging strategy.

RECOMMENDATIONS

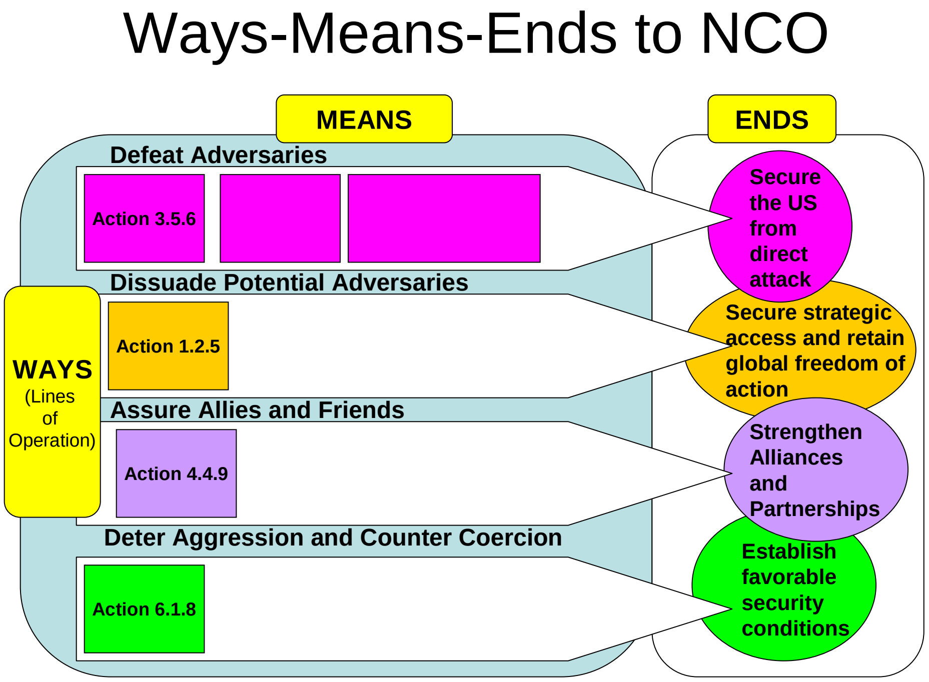
The CCDRs must embed the DISA-owned regional TNCs in the everyday battle rhythm of their respective J3s. The TNC has the resources (tools, capabilities, and personnel skills) to be the TNCC for the CCDR. Figure 7 shows (in red) collapsing the TNCC and TNC under the management of the regional DISA commander, but daily missions and tasks coming from the J3 in support of NCO which includes NetOps functions. The TNC has a dual role derived from tasked TNCC function with the assigned NetOps forces from each of the Service Components. This relationship creates a mirror image between the JTF-GNO and the Service NOSC (OPCON) to the GCC/TNC and assigned Service Theater NOSC.



** In the absence of a STNOSC, the SGNOSC will perform the function of the STNOSC.

Figure 7

Secondly, in order to enhance the realignment, the command relationship between USSTRATCOM and DISA (JTF-GNO) must be replicated at the GCC level with the regional DISA commander (DISA-Europe, DISA-Pacific, etc.). The regional DISA commander must be Senior Rated by the GCC Deputy Commander/Chief of Staff. Finally, the TSC activities, and other exercises must be used as tools to develop net-centric operations tasks that become part of the CCDR's strategy map that support DoD-driven ways, means and ends. Figure 8 below provides a notional GCC Strategy Map. For example, Action 3.5.6 supports "Secure the US from direct attack" by "Defeating Adversaries" in the information domain thru Information Assurance and Computer Network Defense sub-tasks. The GCC Strategy Map is nested with the Service Components to create the value network thru TSC and other training events such as mission rehearsal exercises (MRX).



Ways-Means-Ends to NCO

MEANS

ENDS

WAYS (Lines of Operation)

Defeat Adversaries

Action 3.5.6

Dissuade Potential Adversaries

Action 1.2.5

Assure Allies and Friends

Action 4.4.9

Deter Aggression and Counter Coercion

Action 6.1.8

Secure the US from direct attack

Secure strategic access and retain global freedom of action

Strengthen Alliances and Partnerships

Establish favorable security conditions

Figure 8. Notional GCC NCO Strategy Map

ENDNOTES

1. David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority* 2d ed (Revised) (Washington D.C.: CCRP Publication Series. February 2000), 3.

2. U.S. Department of Defense, The Joint Staff, C2 Capabilities Division, *Joint Command and Control Functional Concept* (February 2004), (Washington D.C., 2004), A5.

3. David S. Alberts and others, *Understanding Information Age Warfare*, (Washington D.C. CCRP Publication Series, August 2001), 60.

4. Vijay Gurbaxani and Robert Plice, *A Model of Network Centric Operations* (Irvine: The CRITO Consortium, July 2004), 2.

5. Ibid., 20.

6. *Star Trek First Contact*. Produced by Rick Berman. Directed by Jonathan Frakes. 111 min. Paramount Pictures, 1996. Videocassette.

7. Vijay Gurbaxani and Robert Plice, *A Model of Network Centric Operations* (Irvine: The CRITO Consortium, July 2004), 1.

8. Ibid., 2.

9. U.S. Department of Defense, Department of the Navy, *The National Defense Strategy of the United States of America*, (Newport, R.I., The United States Naval War College, Joint Military Operations Department, March 2005), 14.

10. U.S. Department of Defense, U.S. Joint Chiefs of Staff. *Doctrine for Joint Operations. Joint Publication 3-0*, (Washington, D.C.: JCS, 10 September 2001), II-3.

11. U.S. Department of Defense, Office of the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer, *Net-Centric Checklist*, *Version 2.1*, 13 February 2004, i.

12. U.S. Department of Defense, *Report on Network Centric Warfare Sense of the Report*, by Arthur L. Money, (Washington D.C. March 2001), 5.

13. David S. Alberts and others, *Understanding Information Age Warfare*, (Washington D.C. CCRP Publication Series, August 2001), 1.

14. Daniel Gonzales and others, *Network-Centric Operations Case Study: The Stryker Brigade Combat Team* (Santa Monica, Calif.: The Rand Corporation, 2005), xiii.

15. U.S. Department of Defense, *Report on Network Centric Warfare Sense of the Report*, by Arthur L. Money, (Washington D.C. March 2001), 5.

16. Daniel Gonzales and others, *Network-Centric Operations Case Study: The Stryker Brigade Combat Team* (Santa Monica, Calif.: The Rand Corporation, 2005), 30.

17. U.S. Department of Defense, *Report on Network Centric Warfare Sense of the Report*, by Arthur L. Money, (Washington D.C. March 2001), 5.

18. Mary Lawlor, "War Validates Netcentricity Concept," *Signal,* November 2005, 18.

19. Ibid., 21.

20. "Lt. Gen. Steven W. Boutelle, USA, Army Chief Information Officer/G-6, talks about how technology is supporting ground forces today and helping the Army transform for tomorrow…," *CHIPS Magazine*, Fall 2003, 20.

21. U.S. Department of Defense, *Report on Network Centric Warfare Sense of the Report*, by Arthur L. Money, (Washington D.C. March 2001), 6.

22. Mary Lawlor, "War Validates Netcentricity Concept," *Signal,* November 2005, 21.

23. Ibid.

24. U.S. Department of Defense, Joint Task Force – Global Network Operations, *500-Day Action Plan for Implementing GIG NETOPS,* by Lt. Gen. Harry D. Raduege, Jr., May 2005, 4.

25. Amy Butler, "DISA Director To Take On New Role As Operational Chief of DoD Networks," *Defense Daily*, 20 February 2004, 4.

26. U.S. Department of Defense, United States Strategic Command, *Joint Concept of Operations for Global Information Grid NetOps*, 24 April 2006, 19.

27. "Joint Staff's New C4 Chief Planning 'Knowledge Management' Doctrine," *InsideDefense.com*, 31 August 2006, 4.

28. U.S. Department of Defense, United States Strategic Command, *Joint Concept of Operations for Global Information Grid NetOps*, 24 April 2006, 11.

29. Ibid., 12.

30. Ibid., 36.

31. Ibid., 23.

32. David S. Alberts and others, *Understanding Information Age Warfare*, (Washington D.C. CCRP Publication Series, August 2001), 95.

33. Ibid., 96.

34. Ibid., 99.

35. Ibid., 101.

36. U.S. Department of Defense, Joint Staff, Command, Control, Communications and Computer (C4) Systems Directorate (J-6), *Joint Communications System Campaign Plan*, July 2006, 8.

37. Ibid., 11.

38. Ibid., 41.

39. Ibid., 48.

40. Ibid., 54.

41. Ibid., 60.

42. Ibid., 66.

43. Moshe F. Rubenstein and Kenneth R. Pfeiffer, *Concepts in Problem Solving*, (Englewood Cliffs, N.J.: Prentice-Hall, 1980), 3.

44. Ibid., 4.

45. U.S. Department of Defense, Joint Staff, Command, Control, Communications and Computer (C4) Systems Directorate (J-6), *Joint Communications System Campaign Plan*, July 2006, 71.

46. Ibid.

47. Vijay Gurbaxani and Robert Plice, *A Model of Network Centric Operations* (Irvine: The CRITO Consortium, July 2004), 1.

48. Ibid., 18.

49. Ibid., 14.

50. Arthur K. Cebrowski and John J. Garstka, "Network-Centric Warfare: Its Origin and Future," *Naval Institute Proceedings Magazine*, January 1998, 5.

BIBLIOGRAPHY

Alberts, David S., John J. Garstka, and Frederick P. Stein. Network Centric Warfare: Developing and Leveraging Information Superiority. 2d ed (Revised). Washington D.C.: CCRP Publication Series. February 2000.

Alberts, David S., John J. Garstka, Richard E. Hayes and David A. Signori. Understanding Information Age Warfare. Washington D.C. CCRP Publication Series. August 2001.

Butler, Amy. "DISA Director To Take On New Role As Operational Chief of DoD Networks." *Defense Daily*, 20 February 2004, 4.

Cebrowski, Arthur K. and Garstka, John J. "Network-Centric Warfare: Its Origin and Future." *Naval Institute Proceedings Magazine,* January 1998, 1-12.

Gonzales, Daniel, Michael Johnson, Jimmie McEver, Dennis Leedom, Gina Kingston, and Michael Tseng. Network-Centric Operations Case Study: The Stryker Brigade Combat Team. Santa Monica, Calif.: The Rand Corporation, 2005.

Gurbaxani, Vijay and Robert Plice. *A Model of Network Centric Operations.* Irvine: The CRITO Consortium, July 2004.

"Joint Staff's New C4 Chief Planning 'Knowledge Management' Doctrine." *InsideDefense.com*, 31 August 2006.

Lawlor, Mary. "War Validates Netcentricity Concept." *Signal* (November 2005) : 17-22.

"Lt. Gen. Steven W. Boutelle, USA, Army Chief Information Officer/G-6, talks about how technology is supporting ground forces today and helping the Army transform for tomorrow…" *CHIPS Magazine*, Fall 2003, 19-21.

Rubenstein, Moshe F. and Kenneth R. Pfeiffer. Concepts in Problem Solving. Englewood Cliffs, N.J.: Prentice-Hall, 1980.

Star Trek First Contact. Produced by Rick Berman. Directed by Jonathan Frakes. 111 min. Paramount Pictures, 1996. Videocassette.

U.S. Department of Defense, Joint Task Force – Global Network Operations. *500-Day Action Plan for Implementing GIG NETOPS*, by Lt. Gen. Harry D. Raduege, Jr. May 2005.

U.S. Department of Defense. The Joint Staff, C2 Capabilities Division. *Joint Command and Control Functional Concept* (February 2004). Washington D.C., 2004.

U.S. Department of Defense. Office of the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer. *Net-Centric Checklist*. *Version 2.1*. 13 February 2004.

U.S. Department of Defense. Department of the Navy. *The National Defense Strategy of the United States of America.* Newport, R.I., The United States Naval War College, Joint Military Operations Department, March 2005.

U.S. Department of Defense. *Report on Network Centric Warfare Sense of the Report*, by Arthur L. Money. Washington D.C. March 2001

U.S. Department of Defense. United States Strategic Command. *Joint Concept of Operations for Global Information Grid NetOps*. 24 April 2006.

U.S. Department of Defense. Joint Staff, Command, Control, Communications and Computer (C4) Systems Directorate (J-6). *Joint Communications System Campaign Plan*. July 2006.

U.S. Joint Chiefs of Staff. Doctrine for Joint Operations. Joint Publication 3-0. Washington, D.C.: JCS, 10 September 2001.