3-16-2007

Strategic Planning to Conduct Joint Force Network Operations: A Content Analysis of NETOPS Organizations Strategic Plans

Antonio J. Scurlock

STRATEGIC PLANNING TO CONDUCT JOINT FORCE NETWORK OPERATIONS:

A CONTENT ANALYSIS OF NETOPS ORGANIZATIONS STRATEGIC PLANS

THESIS

Antonio J. Scurlock, Lieutenant, USN

AFIT/GIR/ENV/07-M18

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

“The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, United States Navy, Department of Defense, or the United States Government.”

AFIT/GIR/ENV/07-M18

STRATEGIC PLANNING TO CONDUCT JOINT FORCE NETWORK OPERATIONS

A CONTENT ANALYSIS OF NETOPS ORGANIZATIONS STRATEGIC PLANS

THESIS

Presented to the Faculty

Department of Systems and Engineering Management

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Information Resource Management

Antonio J. Scurlock, BA, GSEC, MCP

Lieutenant, USN

March 2007

AFIT/GIR/ENV/07-M18

STRATEGIC PLANNING TO CONDUCT JOINT FORCE NETWORK OPERATIONS

A CONTENT ANALYSIS OF NETOPS ORGANIZATIONS STRATEGIC PLANS

Antonio J. Scurlock, BA, GSEC, MCP

Lieutenant, USN

Approved:

/signed/	16 March 2007
Alan R. Heminger, Ph.D. (Chairman)	Date
/signed/	16 March 2007
Dennis D. Strouble, Ph.D. (Member)	Date
/signed/	16 March 2007
Todd A. Peachey, Major, USAF, Ph.D. (Member)	Date

Abstract

Within the Joint Force Network Operations (NETOPS) environment, war fighters will treat net-centric adversaries and global information grid defense-in-depth situations as complex, adaptive enclaves that are the product of the dynamic interactions between connected entities and processes. Because of net centricity, no entity or process of the enclave can be considered in isolation; no singular engagement methodology will accurately capture the enclave's complexity, and an alignment of Department of Defense Combatant Commanders, Services, and Agencies (CC/S/A) strategic planning is pivotal.

To achieve and maintain information dominance, Joint Network Operations (NETOPS) organizations need to be strategically aligned. Strategic alignment allows organizations tasked with conducting NETOPS to meet the needs of the NETOPS Combatant Commander, United States Strategic Command (USSTRATCOM) and as a result, to enhance the capabilities-based effects of NETOPS and reduce our NETOPS infrastructure's susceptibility to compromise.

The goal of this research effort was to answer the question "Are the strategic plans of the organizations tasked with conducting NETOPS aligned?" Once the key organizations were identified, their strategic plans were analyzed using a structured content analysis framework. The results illustrated that the organizations strategic plans were aligned with the community of interests tasking to conduct NETOPS. Further research is required into the strategic alignment beyond the strategic (national/theater) and operational levels to determine if the developed NETOPS strategic alignment construct is applicable to all levels of war.

Acknowledgements

There are many people that were instrumental in the completion of this document. I want to thank my thesis advisor, Dr Alan Heminger, for his patience, feedback, and expert guidance. Thanks to my other committee members, Dr Dennis Strouble, and Major Todd Peachey for their time, patience, and willingness to help with my work.

Thanks to the Office of the Department of the Navy Chief Information Officer (DONCIO) for honoring me with their willingness to sponsor this research effort. Also to Commander, Naval Network Warfare Command (COMNAVNETWARCOM) and the Commander, Navy Global Network Operations and Security Center (COMNAVGNOSC) for their commitment to Joint Network Operations and teaching me the importance of the NETOPS mission to the security of our Nation. I am honored to have served with both commanders.

Thanks to my fellow GIR 07M classmates who selflessly aided me throughout this process, especially my alternate recorder/coder and various members of my “ad hoc” thesis defense committee. Each of these "ad hoc" members put a lot of time and effort into reading and editing my work, and I greatly appreciate their efforts. I give a hearty thanks to each of them for always helping despite the mental anguish and pain they suffered in the process!

Finally, I want to give a very deep thanks to my wife, daughters, and closest friends. Always by my side through thick and thin, they put up with my numerous deadlines and endless hours of work, and yet were always there when I needed them. As always, their love and support are my strength to accomplish all things.

LT Antonio Scurlock

Table of Contents

Page

Page

List of Figures

Figure **Page**

List of Tables

Figure **Page**

STRATEGIC PLANNING TO CONDUCT JOINT FORCE NETWORK OPERATIONS

A CONTENT ANALYSIS OF NETOPS ORGANIZATIONS STRATEGIC PLANS

I. Introduction

Charles de Gaulle said, "[the commander and his troops] must be able to see the situation as a whole, attribute to each object its relative importance, grasp the connections between each factor in the situation, and recognize its limits" (de Gualle, 1934). De Gaulle was speaking to strategic planning, the audience, and the measure of its ability to communicate the way ahead to the individual and the organization. According to the Capstone Concept for Joint Operations (CCJO), August 2005, "all joint force elements will be connected and synchronized in time and purpose to facilitate integrated and interdependent operations across the global battle space" (CJCS, 2005, p. 21). Strategic planning within and across organizations has become critical to conducting operations within the information domain of the global battle space.

The Government Performance and Results Act of 1993 (enacted in 1997), commonly referred to as "GPRA" or "the Results Act," requires federal agencies to submit a strategic plan. The Strategic plan is mandated to contain (OMB, 2006):

> (1) a comprehensive mission statement covering the major functions and operations of the agency; (2) general outcome-related goals and objectives for the functions and operations of the agency; (3) a description of how the goals and objectives are to be achieved (to include a description of operational processes, skills, technology, human capital, information, and any other resources required to

> meet these goals and objectives; (4) a description of how the performance goals included in the plan...shall be related to the general goals and objectives in the strategic plan; (5) an identification of those key factors external to the agency and beyond its control that could significantly affect the achievement of the general goals and objectives; and (6) a description of the program evaluations used in establishing or revising general goals and objectives, with a schedule for future program evaluations. When developing [the] strategic plan, the [agency] shall solicit and consider the views and suggestions of those entities potentially affected by or interested in such a plan (p. 1/2).

Strategic plans determine an organizations way ahead for a determined amount of time. In the case of the GPRA, this timeline is "a minimum six-year period: the fiscal year it is submitted and at least five years forward of that fiscal year" (OMB, 2006, pg 3). The strategic plan details the mission and vision of how an organization is going to get from "here" to "there" and how the organization will know if it got "there" or not. Unlike business plans, which focus on a particular product, service or program, the focus of a strategic plan is usually on the entire organization.

Within the Joint Force Network Operations (NETOPS) environment, war fighters treat net-centric adversaries and global information grid defense-in-depth situations as complex, adaptive enclaves that are the product of the dynamic interactions between connected entities and processes. Because of net centricity, no entity or process of the enclave can be considered in isolation; no singular engagement methodology will accurately capture the enclave's complexity, and an alignment of Department of Defense

Combatant Commanders, Services, and Agencies (CC/S/A) strategic planning is pivotal. To engage in this net-centric war fighting environment and achieve information dominance, the CC/S/A strategic plans must be structured, developed and delivered to meet the vision of the National Security Strategy, National Military Strategy, National Defense Strategy, and keystone documents for communications system support to NETOPS.

NETOPS is an organizational, procedural and technological construct for ensuring information superiority and enabling speed of command for the digital warrior. It links together widely dispersed network operations centers through a command and organizational relationship; establishes joint tactics, techniques and procedures to ensure a joint procedural construct; and establishes a technical framework in order to create a common network picture for the joint force commander (CJCS, 2006b). NETOPS will include all those activities required to monitor, manage and defend and control the Global Information Grid (GIG).

> The Quadrennial Defense Review Report (DOD, 2006b) states that:
>
> "Global Information Grid (GIG) is a globally interconnected, end-to-end set of trusted and protected information networks…[The] GIG optimizes the processes for collecting, processing, storing, disseminating, managing and sharing information within the Department [of Defense] and with other partners" (p. 58).

GIG Overarching Policy (DOD, 2003) establishes policy and assigns responsibilities for GIG configuration management, architecture, and the relationships with the Intelligence Community (IC) and defense intelligence components.

In an age of “information”, where an organization must define its capability to maintain information dominance and conduct NETOPS, strategic plans become the medium through which the digital warrior is connected with think-tanks of senior and executive leadership. This connection allows the digital warrior to fight and defend the NETOPS environment. “In the all-important battle for information superiority, the information domain is ground zero” (OFT, 2003, p. 33). Given that, the purpose of this research is to identify, categorize and synthesize the strategic plans of Department of Defense NETOPS organizations to ascertain the alignment of these strategic plans to key NETOPS concepts, particular emphasis is given to those organizations specifically identified with the role and responsibility for conducting NETOPS by Department of Defense directive or Presidential Executive Order.

Central Research Question

In order to address the purpose of this research, the following research question is posited: “Are the strategic plans of the organizations tasked with conducting NETOPS aligned?”

Scope, Assumptions and Limitations

Goldwater-Nichols Department of Defense Reorganization Act of 1986 (Pub.L. 99-433), the Secretaries of the Military Departments assign all forces to combatant commands except those assigned to carry out the mission of the Services. The chain of command to these Combatant Commands runs from the President to the Secretary of Defense directly to the Commander of the Combatant Command. United States Strategic

Command (USSTRATCOM), is assigned the mission for directing the operations and defense of the GIG. Strategic plans for organizations or entities outside the Department of Defense will only be used in the content analysis if the strategic plan is from an organization that has been directed by higher (above the secretary of defense) authority to conduct NETOPS within the GIG beyond the scope and responsibility of United States Strategic Command (USSTRATCOM). The researcher assumes that draft documents are not authoritative or directive. Draft strategic plans will not be included in the content analysis. Only unclassified strategic plans will be used in the research. Due to time constraints, strategic plans released after January 2007 may not be included in the content analysis. The chief limitation on the researcher and conducting the content analysis will be the designation and availability of strategic plans from various organizations and/or entities. Other than titling, a strategic plan used within the content analysis is considered such of it is designation as a strategic plan from an authoritative source.

Approach/Methodology

A compilation of Strategic Plans, developed by organizations specifically tasked with directing, supporting, planning, and purchasing the capability to conduct Joint Force Network Operations (NETOPS), were collected. This research is an attempt to extract themes from the strategic plans and uncover insights on what this body of text says about conducting NETOPS, the operating, supporting, defending and exploiting the capabilities of the Global Information Grid (GIG).

Thesis Overview

The breath of the research document will detail the efforts to address the research questions listed in this chapter. Chapter II will lay the theoretical foundation of this research work with a thorough review of accessible military literature. Specifically, a general review will be conducted of Global Network Operation Environment within the context of federal, Department of Defense, and Joint training strategy, plans, and policy. Chapter III presents the research methodology used in this study, while Chapter IV sets forth a detailed analysis of the collected data and the findings that resulted from this analysis. Finally, the thesis will close with Chapter V and the presentation of conclusions, limitations, and recommendations for future research. This research is organized in accordance with the American Psychological Association (APA).

II. Literature Review

Introduction

The concept of strategy and strategic planning are nothing revolutionary. Although strategic planning has been taught in business schools since the 1920s, it came into widespread use in the 1970s when the degree of internal and external change to business organizations started increasing at an accelerating rate (Bean, 1993). The focus of a strategic plan is primarily on the entire organization. A well crafted strategic plan determines where an organization is going over a predetermined period of time or engagement, how the organization is going to get there and how the organization will know if the organization achieved it's objectives/goals…or not. In the global network operations environment Department of Defense organizations are forced to develop strategic plans that can accommodate the possibility of change to include, yet not limited to-

1. Rapid technical advances.
2. Stricter government regulations and deregulation.
3. Increasing globalization of the information domain.
4. Decreasing availability of unique resources.
5. Information Assurance
6. Uncertainty

Different strategic-planning methods were developed to help organizations make long-range decisions. Numerical-growth goals were the norm, with the destiny of many

organizations depending on the predictions of the future computed by "ivory tower corporate planning staffs" (Bean, 1993, p. 29).

Strategic planning has evolved to the point that it now views the organization in much broader terms and strives to address the organization's internal strengths, weaknesses, opportunities, and threats (SWOT) in the internal and external environments that have the greatest potential impact on the organization. Strategic planning is war on a map, the literal plan on paper to conduct the engagement at every level of war. Getting from the strategic level of war to the tactical level of war requires an "attention to a number of structural, personnel, and resource issues" (Harvard Business Essentials, 2005, p. 64).

The following literature review gives an overview of the Department of Defenses' Global Information Grid (GIG) and a working definition of the phrase "Joint Network Operations (NETOPS)". It will explore the organization construct for conducting NETOPS within the context of the United States Strategic Commands *Joint Concept of Operations for the GIG NETOPS Version 3* (STRATCOM, 2006). Finally, this chapter will provide a brief synopsis of the relevant organizational structures within the Department of Defense that conduct NETOPS.

Organizational Guidance

Organizational guidance can be formal or informal. Formal guidance is tasking that the organization is required to follow by law or orders from designated authorities. Examples of formal guidance include United States Codes, federal policies or regulations, Department of Defense (DOD) directives, international agreements,

administrative agency manuals, and Joint publications. For well over 15 years, the U.S. Congress has passed legislation that is focused upon creating and sustaining high-performing organizations across the government. This can be seen in the passing of the 1990 *Chief Financial Officers Act* and related financial management legislation; the 1993 *Government Performance and Results Act (GPRA)* and information technology reform legislation, including the 1996 *Clinger-Cohen Act (CCA).*

What has been made clear in these legislative acts passed by Congress, and recommended by the Government Accountability Office (GAO) in their 1999 report entitled "Management Reform: Using the Results Act and Quality Management to Improve Federal Performance", is that the government and entities conducting initiatives with and within the government must focus on developing (GAO, 1999):

1. A clear mission and vision for the organization and a sense of direction that is clearly and consistently communicated by top leadership.
2. A strategic planning process that yields results-oriented program goals and performance measures that flow from and reinforce the organization's mission.
3. Organizational alignment to achieve goals (p. 2).

Informal guidance is typically embodied in norms that are no less binding than the aforementioned legislative acts, such as the separate military services' Core Values, Guiding Principles, and particularly Department of Defense organizations strategic way ahead. Organizational guidance defines the structure, areas of responsibility, and even the environment in which the organization exists (Bryson, 2004).

Global Information Grid (GIG)

All things net-centric have a foundation, a system upon which an organization or other entity is structured at the most basic level. In the private sector this foundation would be the equivalent of large-scale public systems, services, and facilities that are necessary for economic activity, including power and water supplies, public transportation, telecommunications, roads, and schools. Within the Department of Defense, this foundation or infrastructure for all things net centric is the GIG. According to the Department of Defense Dictionary of Military and Associated Terms (short name JP 1-02), the Global Information Grid is (CJCS, 2006b):

> "The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The Global Information Grid includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services and National Security Systems" (p. 227).

General Peter Pace, Chairman of the Joint Chiefs of Staff, established Joint Publication (JP) 6-0, "Joint Communications System", as the "keystone document for communications system support to joint operations [that] provides guidelines to our commanders regarding information systems and networks as a part of the Global

Information Grid" (CJCS, 2006b). This doctrine further expands the definition of the GIG as follows:

> “The GIG supports all DOD, national security, and related intelligence community (IC) missions and functions (strategic, operational, tactical and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms and deployed sites). The GIG provides interfaces to multinational and non-DOD users and systems” (p. viii).

The GIG, due to its broad impact on information capabilities delivery, is often referred to as a weapons system within the network centric operational environment. Like other weapons systems, such as naval air craft carriers, the GIG needs to be able to be operated with impunity and defended from external and internal threats to its operations. JP 1-02 defines these “activities conducted to operate and defend the Global Information Grid” as network operations, or NETOPS.

Joint Force Network Operations (NETOPS)

The Joint Publication (JP) 6-0, "Joint Communications System", has been ten years in the revision process. The global network operational environment has changed considerably since 1995, the last time this keystone document for joint communications was updated. Critical elements of the joint publications revisions are (CJCS, 2006b):

1. Consolidates Joint Publication (JP) 6-02, Joint Doctrine for Employment of Operational/Tactical Command, Control, Communications, and Computer

Systems and JP 6-0 formerly called Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations

2. Discontinues use of the term “command, control, communications, and computers (C4) systems” and replaces it with “communications system”
3. Deconstructs the acronym “C4ISR” into its component parts: “command and control (C2)," "communications system,” and “intelligence, surveillance, and reconnaissance (ISR).” Only the component being discussed is appropriately referenced.
4. Discusses information superiority.
5. Introduces joint force network operations (NETOPS).
6. Introduces network enabled operations (p. iii).

In the simplest of terms, NETOPS is defined as the “mission to operate and defend the [Global Information Grid]” (CJCS, 2006b, pg IV-1). When conducted with precision and effectiveness, “NETOPS provides integrated network visibility and end-to-end management of networks, global applications, and services across the [Global Information Grid]” (CJCS, 2006b, p. IV-1).

Combat has two core tenants that are the keys to consecutively winning engagements, campaigns, operations, and ultimately wars; capabilities and effects. The NETOPS mission, in the context of the GIG, will enable several capabilities; Enhance Joint and Multinational Operations and Interagency Coordination, Provide Strategic Agility, Expand Operational Reach, Increase Tactical Flexibility, Support Network Enabled Operations, and achieve and Maintain Information Superiority (IS). The desired

effects from these capabilities provided by the NETOPS mission are; “assured system and network availability, assured information protection, and assured information delivery” (CJCS, 2006b, p. IV-1). It is these effects that are at the core (Figure 1) of the NETOPS conducted by a special cadre of agencies, commands, and organizations that make up the Joint Network Operations (NETOPS) Community.

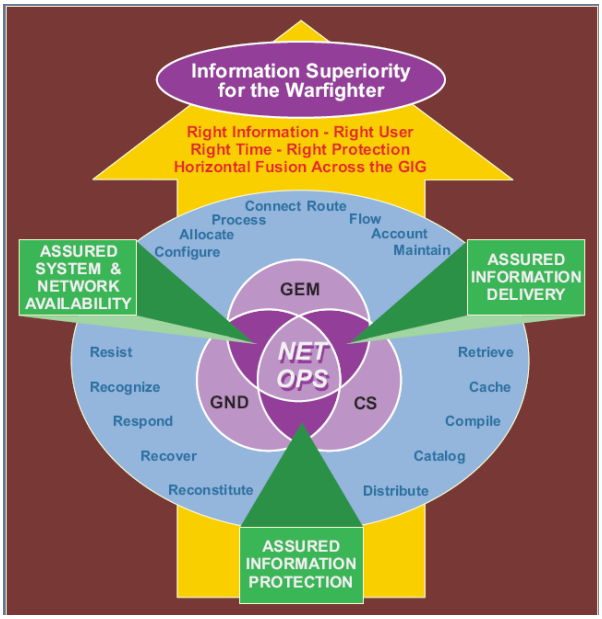

Figure 1 Joint Network Operations (NETOPS) Essential Tasks

The Joint Network Operations (NETOPS) Community

2006 Quadrennial Defense Review (QDR) Report, which is routed in the 2005 National Defense Strategy (NDS), states that the "Assistant Secretary of Defense for Networks & Information Integration [ASDNII], the Department of Defense’s Chief Information Officer, in coordination with [United States Strategic Command], has developed a defense-in-depth strategy for protecting the Department’s computer networks" (DOD, 2006b, p. 50). The enablers of the defense-in-depth strategy are the

Joint Network Operations (NETOPS) Community. This community is comprised of the following commands and agencies:

The Federal Chief Information Officer Council

The Chief Information Officers Council was initially established by *Executive Order (E.O.) 13011, "Federal Information Technology"*. The *E-Government Act of 2002* codified the Chief Information Officers Council (E.O. 13011 was revoked by E.O. 13403, May 12, 2006) as the principal "interagency" [emphasis added] forum to improve agency management of information resources and technology. The Federal CIO Council memberships consist of CIO and Deputy CIO's from the following executive agencies (CIO, 2007):

Department of Labor
Director of National Intelligence
Department of Agriculture
Department of the Air Force
Department of the Army
Department of Commerce
Department of Defense
Department of Education
Department of Energy
Department of Justice
Department of Homeland Security
Small Business Administration
Department of Housing and Urban Development
Agency for International Development
Department of the Interior
Department of the Navy
Department of State
Department of Transportation
Department of the Treasury
Department of Veterans Affairs
Environmental Protection Agency
General Services Administration
Social Security Administration
National Science Foundation
Nuclear Regulatory Commission
Office of Personnel Management
Department of Health and Human Services
National Aeronautics and Space Administration

According to the CIO Council Charter, the council was "established to achieve information resource management (IRM) objectives delineated in legislation including

the *E-Government Act of 2002 (Public Law 107-347)*, *Government Paperwork Elimination Act (GPEA)*, *Paperwork Reduction Act (PRA)*, *Government Performance and Results Act (GPRA)*, and the *Information Technology Management Reform Act of 1996 (ITMRA)*" (CIO, 2003).

The Assistant Secretary of Defense for Networks & Information Integration

The Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer (ASD(NII)/DOD CIO), per Department of Defense Directive 5144.1 (DOD, 2005a), is the;

1. Serve as the senior NII and CIO policy and resources official below the Secretary and Deputy Secretary of Defense. (par. 3.1)
2. Lead the formulation and implementation of enterprise-level defense strategies from the information, IT, network-centric, and non-intelligence space perspective. (par. 3.3.2)
3. Serve as the DOD-wide information executive and participate as a member on DOD-wide councils and boards involving NII and CIO matters, including serving as the DOD representative on the Intelligence Community CIO Executive Council. (par. 3.3.5)
4. Chair the DOD CIO Executive Board. (par. 3.3.21) "The DOD CIO Executive Board is the principal forum used to advise the DOD CIO on the full range of matters pertaining to the GIG. It also coordinates implementation of activities under the Clinger-Cohen Act of 1996, and exchanges pertinent information

and discusses issues regarding the GIG, including DOD IM and IT" (CJCS, 2006b, pg II-18).

5. Provide policies, oversight, guidance, architecture, and strategic approaches for all communications and information network programs and initiatives on an enterprise-wide basis across the Department, ensuring compliance with the IA requirements as well as interoperability with national and alliance/coalition systems. This includes network-centric and information-integration projects, programs, and demonstrations as they relate to GIG implementation and employment. (par. 3.4.3)

The ASD(NII)/DOD CIO also has the responsibility of being the architect of a Department of Defense wide framework for a joint, interagency, integrated infrastructure that DOD will build upon and mandate compliance with National Security Systems (NSS) and Information Assurance (IA) directives.

Chairman of the Joint Chiefs of Staff

The *Goldwater-Nichols Act* directed the Chairman to assist the President and the Secretary of Defense in providing strategic direction to the armed forces. The Chairman's mechanisms for providing advice regarding strategic direction are the Chairman's Guidance, Joint Vision Documents, and National Military Strategy. The Chairman is ultimately responsible for developing joint policy.

Title 10 U.S. Code (Chairman: functions, 2006)assigns to the Chairman two distinct functions regarding strategic planning: Section 153(a)(2) charges the Chairman with "preparing strategic plans, including plans which conform to resource levels

projected by the Secretary of Defense to be available for the period of time for which the plans are to be effective." Section 153(a)(3) makes the Chairman responsible for "providing for the preparation and review of contingency plans which conform to policy guidance from the President and the Secretary of Defense."

The *Unified Action Armed Forces (UNAAF)* is one of two foundation documents for all joint publications. The UNAAF provides the basic doctrine and policy governing the unified direction of forces and discusses the functions of the Department of Defense and its major components. In accordance with the UNAAF, the Chairman of the Joint Chiefs of Staff acts as the "spokesman for the combatant commanders, especially on the operational requirements of their commands" (CJCS, 2001a, p. II-5).

Joint Community Warfighter Chief Information Officer (JCWCIO)

The Director for Command, Control, Communications, and Computer (C4) Systems for the Joint Staff (J6) "Serve as one of the four [Defense Information System Network (DISN)] [Designated Approval Authorities] and exercise authority for operational DISN policy and direction" (CJCS, 2003). The J-6 is designated as the [Joint Community Warfighter (JCW) Chief Information Officer (CIO)] and is tasked with "acting on behalf of the Chairman of the Joint Chiefs of Staff as prescribed in Department of Defense Directives *8000.1, "Management of DOD Information Resources and Information Technology"* (DOD, 2002), and *8100.1, "Global Information Grid (GIG) Overarching Policy"* (DOD, 2003).

United States Strategic Command (USSTRATCOM)

According to the *Joint Concept of Operation for GIG Network Operations Version 3.0* (STRATCOM, 2006), United States Strategic Command (USSTRATCOM) has overall responsibility for Global Network Operations (GNO) and defense of the GIG in coordination with CJCS and the other combatant commands (STRATCOM, 2006). USSTRATCOM is responsible for integrating and coordinating DOD NETOPS capabilities across all geographic Areas of Responsibility (AOR). The *Joint Publication (JP) 6-0, "Joint Communications System"*, states that USSTRATCOM is responsible for advocating “for national requirements and standards, and in coordination with other CCDRs [Combatant Commanders], assess and report the operational readiness of the GIG systems/networks" (CJCS, 2006b, p. II-21/22).

The Military Service Chief Information Officers (CIO)

The *Paperwork Reduction Act of 1995 (PRA) (Title 44 United States Code Sections 3501-3520)* requires each federal agency to designate a Chief Information Officer (CIO) to ensure compliance with federal information policies and implement Information Resource Management to improve agency productivity, efficiency, and effectiveness. Subsequent legislation has refined and expanded these information policies and CIO responsibilities, including the management of Information Technology investments and acquisitions in compliance with the *Clinger-Cohen Act of 1996 (CCA)* (specifically title 40 U.S.C. sections 11101-11704); ensuring that Information Technology and National Security Systems are interoperable and compliant with federal

and Department of Defense standards (specifically title 10 U.S.C. sections 2222 and 2223); and the management and promotion of electronic government services in accordance with the *E-Government Act of 2002* (specifically title 44 U.S.C. section 3501 note, and sections 3601-3606). Additional requirements and guidance are established by the Office of Management and Budget (OMB), and promulgated through *OMB Circular A-130, "Management of Federal Information Resources"* (OMB, 2000).

Army Chief Information Officer (CIO)/G-6

Army Regulation 25-1, "Army Knowledge Management and Information Technology Management", 15 July 2005 tasks the Office of the Army Chief Information Officer (CIO/G-6) with providing architecture, governance, portfolio management, strategy, C4 IT acquisition oversight and operational capabilities to enable joint expeditionary net-centric information dominance for the Army. The regulation requires the Army CIO to oversee and direct the Network Enterprise Technology Command (NETCOM)/9th Army Signal Command. The Army CIO/G-6 reports directly to the Secretary of the Army (Army, 2005).

Department of the Navy (DON) Chief Information Officer (CIO)

Secretary of the Navy (SECNAV) Instruction *5430.7N, "Assignment of Responsibilities and Authorities in the Office of the Secretary of the Secretary of the Navy"*, 9 June 2005 tasks the Department of the Navy Chief Information Officer (DON CIO) as the Secretary of the Navy's principal advisor on Information Management (IM), Information Technology (IT), Information Resource Management (IRM), and National

Security Systems (NSS). The instruction specifically states that, “the DON CIO has sole responsibility for the IM function within the Office of [Secretary of the Navy], the Office of [Chief of Naval Operations], and [Head Quarters Marine Corp]”, and that “no other office or entity may be established to perform these responsibilities” (DON, 2005a). The DON CIO is supported by Deputy CIO’s for the Navy (Deputy Chief of Naval Operations for Communication Networks (N6)) (DON, 2006) and Marine Corps (Director for Command, Control, Communications and Computers (C4), Headquarters Marine Corps (HQMC)) (DON, 2003), and a Deputy CIO for Policy and Integration. The DON CIO reports directly to the Secretary of the Navy.

Warfighter Integration/Chief Information Officer (SAF/XC)

On May 10, 2005 the Secretary of the Air Force Office of Warfighting Integration and Chief Information Officer (SAF/XC) was officially created. The new organization combines three previous entities; the Deputy Chief of Staff, Warfighting Integration (AF/XI), Air Force Chief Information Officer (AF-CIO), and Deputy Chief of Staff, Installations and Logistics (AF/ILC). *Air Force policy directive (AFPD) 33-1, "Information Resource Management"*, 27 June 2006, designates SAF/XC as the principal authority on Department of the Air Force Information Resource Management (IRM), Business Processes (BP), Information Technology (IT), and National Security Systems (NSS) standard (USAF, 2006). The SAF/XC reports to the Secretary of the Air Force, as the Chief Information Officer. The SAF/XC reports to the Chief of Staff of the Air Force as the Warfighting Integrator (SAF/XC, 2006).

The Intelligence Community (IC)

The Intelligence Community (IC) is responsible for those portions of the GIG that are uniquely within the IC domain. The Department of Defense (DOD) Chief Information Officer (CIO) *Guidance and Policy Memorandum, number 11-8450 (2001), "Department of Defense Global Information Grid Computing,"* (DODCIO, 2001) directs that:

1. Co-designate, with the DOD CIO, a select set of computing capabilities and services, to include all SCI networks, to be defined as the IC portion of the GIG (par. 5.5.1).
2. Develop, maintain, and enforce the IC portion of the GIG Architecture (par. 5.5.2).
3. Consult, where appropriate, with the DOD CIO on matters of GIG policy, acquisition, implementation, and operation (par. 5.5.3).

The IC portion of the GIG supports IC operations within the Sensitive Compartmented Information (SCI) environment.

Defense Information Systems Agency (DISA)

The Defense Information Systems Agency (DISA) "is a Defense Agency under the authority, direction, and control of the ASD(NII)/DOD CIO" (DOD, 2005a). The Director of DISA is also designated as the Commander, Joint Task Force-Global Network Operations (JTF-GNO) (DOD, 2005a). *Department of Defense Directive 5105.19, "Defense Information Systems Agency (DISA)"*, July 25, 2006 authorizes DISA

field organizations to exercise operational direction over the Defense Information Systems Network (DISN) operating elements.

Of particular note is the mission assigned to the DISA (DOD, 2006a):

> "The DISA shall be responsible for planning, engineering, acquiring, testing, fielding, and supporting global net-centric information and communications solutions to serve the needs of the President, the Vice President, the Secretary of Defense, and the DOD Components, under all conditions of peace and war [underline emphasis added]".

With the exception of the military services and the Chairman of the Joint Chiefs of Staff, no singular NETOPS entity has responsible for planning, engineering, acquiring, testing, fielding, and supporting global net-centric information and communications solutions to the degree that the DISA does.

Commander, Joint Task Force Global Network Operations (JTF-GNO)

Lieutenant General Robert M. Shea, while serving as the Director, Command, Control, Communications and Computer Systems (C4) systems), The Joint Staff (J-6) said, "U.S. Strategic Command's (USSTRATCOM) Joint Task Force-Global Network Operations (JTF-GNO) is responsible for the policy, guidance, and oversight that will transform today's Department of Defense's (DOD) information assets" (Shea, 2006, p. 18).

Department of Defense Directive (DODD) 5105.19, "Defense Information Systems Agency (DISA)"(DOD, 2006a), authorizes Commander, JTF-GNO to "isolate, disconnect, and/or shutdown information systems (including websites) owned, operated,

sponsored, or funded by the Department of Defense that are in violation of applicable security policies, when so directed by appropriate authority in accordance with established procedures" (DOD, 2006a). The *Joint Concept of Operation for GIG Network Operations Version 3.0* states that "JTF-GNO provides the DOD with the direction and oversight to operate and defend the GIG" (STRATCOM, 2006).

Change 3 to the *Chairman of the Joint Chiefs Staff instruction (CJCSM) 6510.01D, 08 March 2006, "Information Assurance (IA) and Computer Network Defense (CND),"* lists the Commander, JTF-GNO responsibilities as (CJCS, 2006a):

1. [Assessing] operational impacts of possible COAs [Course of Actions] and weigh actions against the risk assessments to preserve the Global Information Grid (GIG). (Annex A, Appendix B, Enclosure B, p. 2)
2. Perform global incident/intrusion monitoring and detection, strategic vulnerability analysis, system forensics, media analysis, and responses to information assurance (IA)/CND-related activity. (Annex A, Appendix B, Enclosure B, p. 3)
3. Coordinate with the [combatant commands, Services and Agencies] C/S/As and field activities in determining the technical and operational mission impacts caused by degradations, outages, and IA and CND events. (Annex A, Appendix B, Enclosure B, p. 3)
4. Coordinate with the Department of Homeland Security (DHS) for all incidents that involve the Department of Defense and other federal agencies. (Annex A, Appendix B, Enclosure B, p. 3)

Joint Task Force-Global Network Operations (JTF-GNO) is the focal point for all combatant commanders, services, and agencies to conduct Joint Network Operations (NETOPS).

Service NETOPS Component Commands

Each of the military services has appointed a component to USSTRATCOM for coordination effort with JTF-GNO and to exercise command and control of their respective Service Global Network Operations and Security Centers (SGNOSC). The Service NETOPS Component Commanders are:

1. Commander, Strategic Missile Defense Command (SMDC)/Army Strategic (ARSTRAT) Command. Commanding General, Army Network Enterprise Technology Command (NETCOM)/9th Signal Command (Army) is the ARSTRAT Deputy for NETOPS and is the single authority assigned to operate, manage, and defend the Army's infrastructure at the enterprise level (NETCOM, 2006).
2. The US Air Force Commander for USAF NETOPS (USAF NETOPS/ CC). The 67th Network Warfare Wing, of the 8th Air Force, is tasked to "execute [Air Force] network operations, defense, attack, and exploitation to create integrated cyberspace effects for Air Force Network Operations Commander and combatant Commands (67NWW, 2006).
3. Commander, US Navy Network Warfare Command (USN NAVNETWARCOM), as the service component commander, exercises Operational Control (OPCON) over the Navy’s Global Network Operations

and Security Center (GNOSC), which is responsible for operational and technical support to the Navy's portion of the GIG (NNWC, 2006b).

4. Commander, US Marine Corps Network Operations and Security Command (MCNOSC). "The Marine Corps Network Operations and Security Command (MCNOSC) is responsible for managing Marine Corps global network operations and Computer Network Defense (CND) of the Marine Corps Enterprise Network (MCEN)" (MCNOSC, 2006).

The command and control relationships of the service component NETOPS entities in relation to JTF-GNO are show in Figure 2 (STRATCOM, 2006, p. 24).

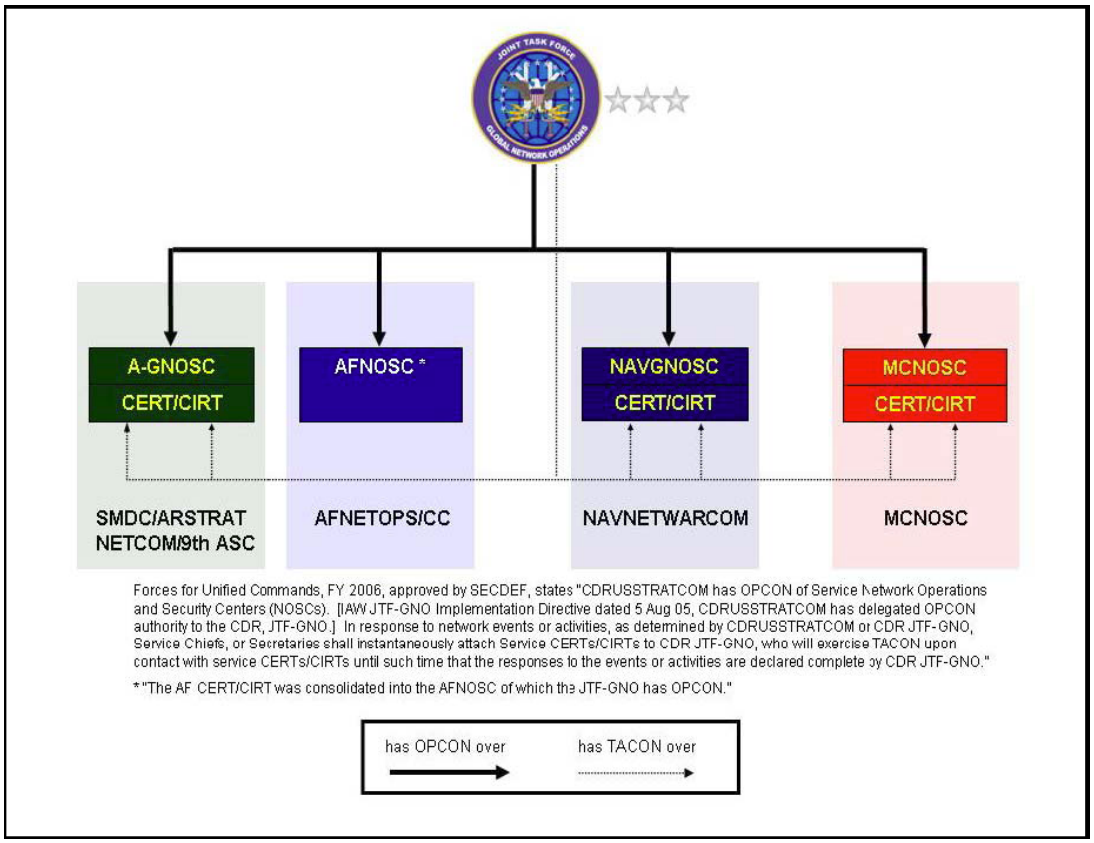

Figure 2 Service Network Operations Components C2 Relationships

Summary

This literature review has provided the foundations for moving towards answering the authors' central research question "Are the strategic plans of the organizations tasked with conducting NETOPS aligned?" The focus of this chapter was to provide the reader with a basic conceptual understanding of the Global Information Grid (GIG), Joint Network Operations (NETOPS), and the organizational entities that conduct NETOPS within the context of the Department of Defenses' Global Information Grid. The next chapter will discuss the methodology that was applied in an attempt to answer the research question.

III. Methodology

Introduction

The purpose of this research is to answer the central research question: "Are the strategic plans of the organizations tasked with conducting NETOPS aligned?" This chapter defines the strategic concept of being aligned. This chapter also defines and details the steps taken in locking onto a methodology and gives follow-on researchers guidance on using this methodology, and it's appropriateness for this type of research.

The research began with an initial literature review of Global Information Grid (GIG) policy, doctrine, directives and instructions to establish a framework for the research. There were a plethora of policy, doctrine, directives and instructions assigning responsibility, authority, and accountability for various function of performing NETOPS – the actions taken to operate and defend the GIG (CJCS, 2006b). Tasking within the various GIG policy, doctrine, directives and instructions was largely to organizations or positions within organizations. Even those documents that assigned responsibility and accountability to multiple entities for developing direction and strategy were not directed beyond the scope of the organizations or positions they were tasking. Where the policy, doctrine, directives and instructions assigned responsibility for providing direction or strategic planning, the researcher noticed that there did not seem to be any further guidance other than to generate, not necessarily to coordinate, a strategic document with various elements within the context of GIG NETOPS. The apparent lack of more specific guidance on context and coordination prompted the question: "Are the strategic plans of the organizations tasked with conducting NETOPS aligned?" Robert S. Kaplan and David P. Norton (2006) define "alignment" as "all units, process, and systems of an organization linked to [the organizations] strategy (p. 259).

Qualitative Research

Leady and Ormrod (2005) state that “to answer some research questions…we must dig deep to get complete understanding of the phenomenon we are studying” (p. 133). The nature of conducting NETOPS is people, processes, and technology working together to enable timely and trusted access, sharing, and collaboration of information to any and all that need it. The variations and multifaceted aspects of NETOPS and the governing strategy’s that guide the conducting of NETOPS are perfectly suited for a qualitative study. The study of strategy and strategic plans of conventional warfare environments is nothing knew. The study of strategy and the strategic plans of the organizations conducting information-age warfare are currently unprecedented. In situations where there is a lack of clarity or understanding of a particular concept or phenomenon, Cresswell espouses the use of a qualitative methodology (Cresswell, 2003). The contextual properties of strategic plans, by definition are a proxy for [future] experience that may be inferred from the body of free-flowing texts coding (Denzin & Lincoln, 2000) and therefore the most appropriate methodology for this research is a content analysis.

Content Analysis

When a researcher is “inquiring into a social reality that consists of inferring features of a non-manifest context from features of a manifest text”, then content analysis is the methodology to use (Krippendorff, 2004, p. 25). Leedy and Ormrod (2005) defines content analysis as a “detailed and systematic examination of the contents of a particular body of material for the purpose of identifying patterns, themes, or biases” (p. 142). Neuendorf (2002) states that “the goal of content analysis is to identify and record relatively objective (or at least intersubjective) characteristics of messages..." (p. 141). The view of content analysis, as defined by Holsti (1996), "any technique for making inferences by objectively and systematically identifying

specified characteristics of messages" (p. 14) takes the methodology out the realm of just textual analysis to other medium of communication. Yet, in order for the methodology to be replicable, to can only be applied to data that is durable. Most human beings draw conclusions from observations of various types of content informally on a daily basis during our multitude of communications with each other. The content analysis methodology, when placed within a research framework, is formal system of what, as aforementioned, people do daily.

Krippendorff (2004) provides a conceptual framework that is prescriptive, analytical, and methodological that guides the “conceptualization and design of the research [that can] facilitate the critical examination and comparison of the published content analysis, [as well as] point to performance criteria and precautionary standards that researchers can apply in evaluating [other] content analysis” (p. 30).

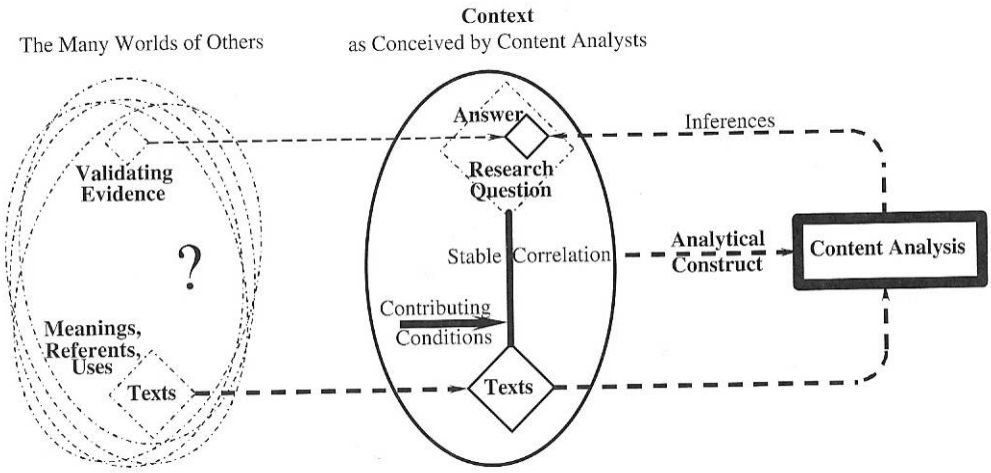

Figure 3 Framework - Conceptual (P.A.M.)

The components of Krippendorff’s (2004) framework are:

1. A body of text, the data that a content analysis has available to begin an analytical effort

2. A research question that the analyst seeks to answer by examining the body of text
3. A context of the analyst's choice within which to make sense of the body of text
4. An analytical construct that operationalizes what the analyst knows about the context
5. Inferences that are intended to answer the research question, which constitute the basic accomplishment of the content analysis
6. Validating evidence, which is the ultimate justification of the content analysis (p. 30-40)

As Figure 3 represents the conceptualized content analyst; it can be seen to contain Figure 4, which represents a simplified content analysis design for comparing similar phenomena inferred from different texts (Krippendorff, 2004, p. 94).

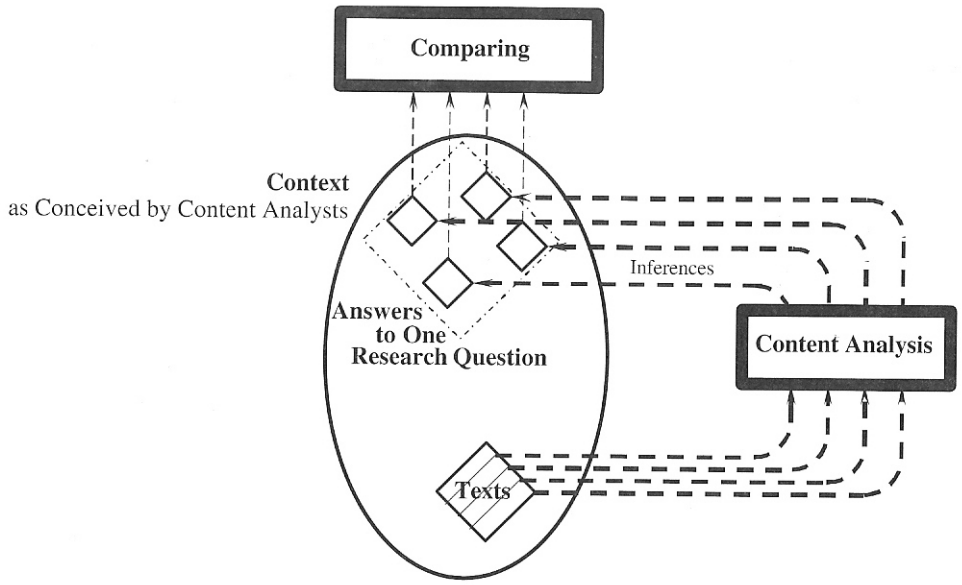

Figure 4 Framework - Simplified Analysis Design

This design is ideal when distinctions from a body of text have the same content analysis applied to them. Specifically the inferences that will be compared are of more significance than the textual make-up of the body of text.

The body of texts and research question were covered in Chapter I. Chapter II provided the context of usage for the body of text within which to make sense of the body of text. The texts, within the context of their use, "acquire significance (meanings, contents, symbolic qualities, and interpretations)" (Krippendorff, 2004, p. 33). The analytical construct will be discussed further in sections of this chapter.

Detailed Components of the Content analysis

An exploded view of the "Content Analysis" box in Figures 3 and Figure 4, is shown in Figure 5. Descriptions of the elements of the components of the "Content Analysis" box will also serve as instructions for replicating the content analysis in future research endeavors.

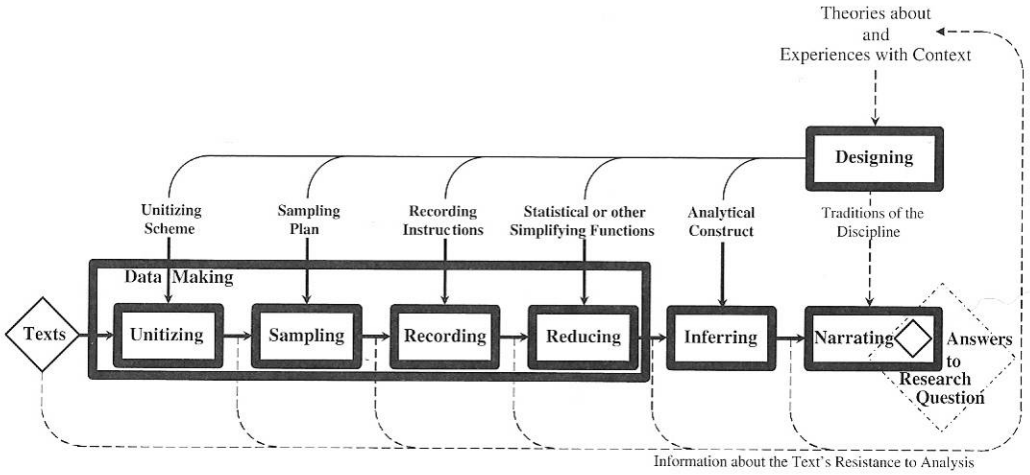

Figure 5 Framework - Components of Content Analysis

Krippendorff (2004) states that each element "has a descriptive and an operational state" (p. 83. The elements are unitizing, sampling, recording/coding, reducing, inferring, and narrating. The inferring and narrating elements will be covered in Chapter IV. The sub elements of the "Data Making" segment of the framework are detailed in the following paragraphs.

Unitizing

The units of analysis for the content analysis are broken into three components: Sampling Units, Context Units, and Recording/Coding Units. Sampling Units are "distinguished for selective inclusion [and possible exclusion] in an analysis (Krippendorff, 2004, p. 99). The Sampling Units for this content analysis are the Strategic Plans of the organizations with the role and responsibility for conducting NETOPS in accordance with Department of Defense Directives, Instructions, Doctrine and Concepts of Operations (CONOPS).

The Context Units are "units of textual matter that set limits on the information to be considered in the description of recording units" (Krippendorff, 2004, p. 101). The Context Units for this content analysis are the mission statements, goals, and objectives detailed within the Strategic Plans of the organizations with the role and responsibility for conducting NETOPS in accordance with Department of Defense Directives, Instructions, Doctrine and Concepts of Operations (CONOPS)

Recording/Coding Units are "units distinguished for separate description, transcription, recording, or coding" (Krippendorff, 2004, p. 99). The Recording/Coding Units for this content analysis are thematic elements regarding NETOPS in mission statements, goal, and objectives detailed within the Strategic Plans of the organizations with the role and responsibility for

conducting NETOPS in accordance with Department of Defense Directives, Instructions, Doctrine and Concepts of Operations (CONOPS).

Sampling

Of the various methods of sampling available, the author chose to use "Relevance Sampling" (Krippendorff, 2004, p. 119) for determining the textual units that would be used within the content analysis for answering the research question. Because the researcher handpicks textual units to analyze in the study based upon identified variables under consideration, Relevance Sampling is closely identified with Purposive Sampling. The identified variables are the Department of Defense Directives, Instructions, Doctrine and Concepts of Operations (CONOPS) that govern NETOPS. When the population for study is highly unique, it is feasible for the researcher to follow a conceptual (or considering context, a mandated) hierarchy, thereby reducing the number of textual units. Krippendorff (2004) states that "Relevance Sampling selects relevant data in ways that statistical sampling theory has not yet addressed" (p. 120).

Recording/Coding

The Recoding/Coding schema are ways that the content analyst records/codes transient, unstructured, or fuzzy but otherwise meaningful phenomena into a medium suitable for subsequent data processing. A search for recording/coding precedence for analyzing strategic plans for alignment was conducted, and no research effort was found to have been performed. The Recording/Coding scheme devised is adapted from a theory presented in congressional testimony by the Government Accountability Office (GAO) (1998) on "[strategic alignment]

challenges that remain to be addressed" (GAO, 1998, p. 3). GAO theorized two key elements of strategic plans that would be needed to meet the [strategic alignment] challenges identified; (1) clearly articulated strategic direction – the document specifically identifies and is organized to describe areas for focus where the organization deems actions are necessary to conduct Joint Force (Interagency) Network Operations (NETOPS) and/or Net-Centric Operations/Warfare (NCOW) and achieve the affects of successfully conducted NETOPS, and (2) the coordination of crosscutting efforts – the document specifically discusses Joint/Interagency coordination for the crosscutting programs, mission-related activities, or functions that are similar to those of other Department of Defense Components and or Federal agencies that conduct NETOPS. For each strategic plan recorded, the coder was asked to analyze the strategic plan and assess the vision/mission statement, general goals and objectives, and approaches or strategies to achieve the goals and objectives. An binary coding scheme was created as shown below:

1 Aligned – Strategic Plan of C/S/A is aligned to conduct NETOPS

0 Not Aligned – Strategic Plan of C/S/A is not aligned to conduct NETOPS

If the strategic plan clearly contained the two key elements, as fully defined above, then the coder was asked to record the strategic plan accordingly and annotate examples. If the strategic plan did not clearly contain the two key elements, as fully defined in the coder training, then the coder was asked to record the strategic plan accordingly with annotated coder comments.

The primary researcher independently coded all of the strategic plans in this body of text and recorded/coded the results within a Microsoft Excel spreadsheet (see Appendix B: "Sample Codebook"). An alternate coder also independently coded all of the strategic plans in this body of text and recorded/coded the results within a Microsoft Excel spreadsheet (see Appendix B: "Sample Codebook"). The alternate recorder/coder was allotted 96 hours to conduct

recording/coding on the body of text. The independent coding efforts are crucial to prevent invalidation of the data due to collaborative coding.

Recorder/Coder Training and Preliminary Reliability

"It is typical for content analyst to provide coders with additional training in using the recording/Coding instructions" (Krippendorff, 2004, p. 129). The alternate recorder/coder was a female GS-15 (Army Colonel/Navy Captain/O-6 equivalent for order of precedence) volunteer from the Army Assistant Chief of Staff for Installation Management (ACSIM). The alternate recorder/coder is currently pursuing a master's degree in National Security Resource Strategy, with a concentration in Information Operations (IO), at the Industrial College of the Armed Forces (ICAF) located at the National Defense University (NDU). The alternate recorder/coder also possesses a diverse background in Information Resource Management (IRM), Portfolio Management and is a Certified Chief Information Officer (CIO).

Two hours (total) of training sessions were conducted with the alternate recorder/coder by the primary researcher. The primary researcher explained the abstract of the thesis research. The alternate recorder/coder was provided an initial definition of alignment. The alternate recorder/coder was also provided with the GAO report that expanded the alignment definition to strategic alignment and was adapted to develop the coding scheme. The alternate recorder/coder was familiarized with the coding scheme as well as the Sampling Units, Context Units, and Recording/Coding Units. After the initial one hour training session, the alternative recorder/coder was provided a sample text and asked to independently code the text. The alternate recorder/coder was allotted 24 hours to code the sample text. The second hour of the recorder/coder training was spent ensuring that both the primary researcher and alternate

recorder/coder understood the fundamentals of the coding scheme. No adjustments to the research question or methodology were made as a result of these training sessions.

Final Reliability

A final measure of reliability will be a comparison of the primary researcher and alternate recorder/coder data/themes. The primary researcher and alternate recorder/coder reviewed the same body of texts. A percentage agreement between the primary researcher and the alternate recorder/coder will be the measure used to calculate reliability. Krippendorff's (2004) **α** will be used to check reliability. Krippendorff's **α** is:

1. Applicable to any number of values per variable and it's correction for chance makes **α** independent of this number
2. It is applicable to nominal, as well as other scales of measurement (p. 222)

Tabulation and Reporting

The results from each coder, primary and alternate were recorded within the Microsoft Excel spreadsheet (see Appendix B: "Sample Codebook"). The data was sorted in multiples ways. Initially, the primary researcher recording/coding was tabulated. Second, the alternate researcher recording/coding was tabulate. Third, the primary researcher and alternate recorder/coder data were combined. The spreadsheet data will be graphically displayed on charts to represent the data and identify associate comments and annotations.

Summary

Krippendorff (2004) provides a conceptual framework that is prescriptive, analytical, and methodological (p. 30). Given the context and textual content of the Sampling Units, Context Units, and Recording/Coding Units, the content analysis methodology provides the best method of answering the primary research question. This conclusion is confirmed by various authors: Leady & Ormrod, Cresswell, Denzin & Lincoln, and Neuendorf (Leady, 2005; Denzin & Lincoln, 2000; Cresswell, 2003; Neuendorf, 2002). The steps used in the analytical construct for conducting the content analysis methodology lead to an unbiased volume of literature to research.

As the primary researcher is an instrument in the conducting of the content analysis, the study is subject to the knowledge, skills, abilities, and any biases possessed by the primary researcher. The next chapter will discuss the results and analysis of the collected, and recorded, data in an attempt to answer the research question.

IV. Results & Analysis

Introduction

This chapter describes the keys themes and concepts discovered during the content analysis of the selected body of text relating to NETOPS Strategic Plan alignment. As articulated in the initial chapter, the objective of this study was to answer the posited question using an exploratory content analysis methodology: "Are the strategic plans of the organizations tasked with conducting NETOPS aligned?" The focus of this question is to define the elements of being strategically aligned within the Joint Network Operations (NETOPS) arena. It is expected that once the themes are presented/re-articulated to answer the research question, that further research will be conducted using the data acquired from this research study to create a codified Joint Network Operations (NETOPS) strategic alignment model which can be applied in the operational leadership, education, and training environment.

The following sections of this chapter discuss the framework and steps used the type of data recorded/coded, and how the results of the research answer the research question above. The first section deals with the primary researcher results, describing the data collection technique and the analysis of the findings. The next section presents the alternate recorder/coders data collection and the analysis of their results. Lastly, the final section provides a correlated view of the primary researches results with the alternate recorder/coder results, and answering the posited research question.

Percent agreement, using Krippendorff's Alpha (**α**), was used to check content validity. The algorithm between the primary researcher and the alternate recorder/coder was calculated for all strategic plans analyzed.

Primary Researcher Data

A loose criteria search for documents associated with Network Operations and Global Information Grid operations, resulted in over 100 documents consisting of United States Codes, federal policies or regulations, Department of Defense (DOD) directives and instructions, international agreements, administrative agency manuals, Joint publications, XXX-Day plans, and strategic documents of various types from multiple entities As a result of this loose criteria, many items contained in the initial dataset was not remotely or directly applicable to the topic of this research. The data-set was narrowed according to the criteria as outlined in Chapter I and the sampling techniques detailed in Chapter III. This process reduced the amount of researcher bias by removing the researcher from the sampling decision for the analyzed data-set.

The primary researcher performed a thorough analysis of the resulting sample, analyzing for any thematic pattern that may be present within each strategic plan. Each theme discovered was recorded for comparison to the perspective themes that may have been discovered by the alternate recorder/coder and therefore be correlated with the primary researchers' discovered themes. Each strategic plan that contained the required elements for alignment was recorded/coded according to an *A Priori* binary coding scheme, as defined in Chapter III as shown below:

1 Aligned – Strategic Plan of C/S/A is aligned to conduct NETOPS

0 Not Aligned – Strategic Plan of C/S/A is not aligned to conduct NETOPS

The independent primary researcher analysis resulted in list of primary categorical Network Operations (NETOPS) entities, organizations, or levels within organizations of significance. The primary categorical Network Operations (NETOPS) entities, organizations, or levels were not ranked, yet they were tabulated based upon authorship and organizational

responsibility for the content of the strategic plan. This resulted in the following table of primary categorical Network Operations (NETOPS) entities, organizations, or levels.

Network Operations Entities
Departmental Level (Overarching – DoD)
Joint War Fighting Community (CJCS/J-6)
Chief Information Officers (Army/Navy/AF/USMC)
Joint Network Operations (JTF-GNO, USSTRATCOM)
Service Network Operations (Army/Navy/AF/USMC)
Intelligence Community (DoD, Service, Federal)
Agency Network Operations (Federal, Non-DoD)
Coalition Network Operations (Partner)

Table 1 Primary Researcher NETOPS Entities

As shown by Table 1, these entities, along with their being tasked with NETOPS by directive, law, or policy, also produce policy, directive, and most importantly strategy to conduct NETOPS appear to be prevalent within all of the strategic plans analyzed. These entities', although not specifically named, correspond with the *Joint Concept of Operations for Global Information Grid Network Operation Version 3* (STRATCOM, 2006, p. 14) command and control structure for a global network operations event (Figure 6).

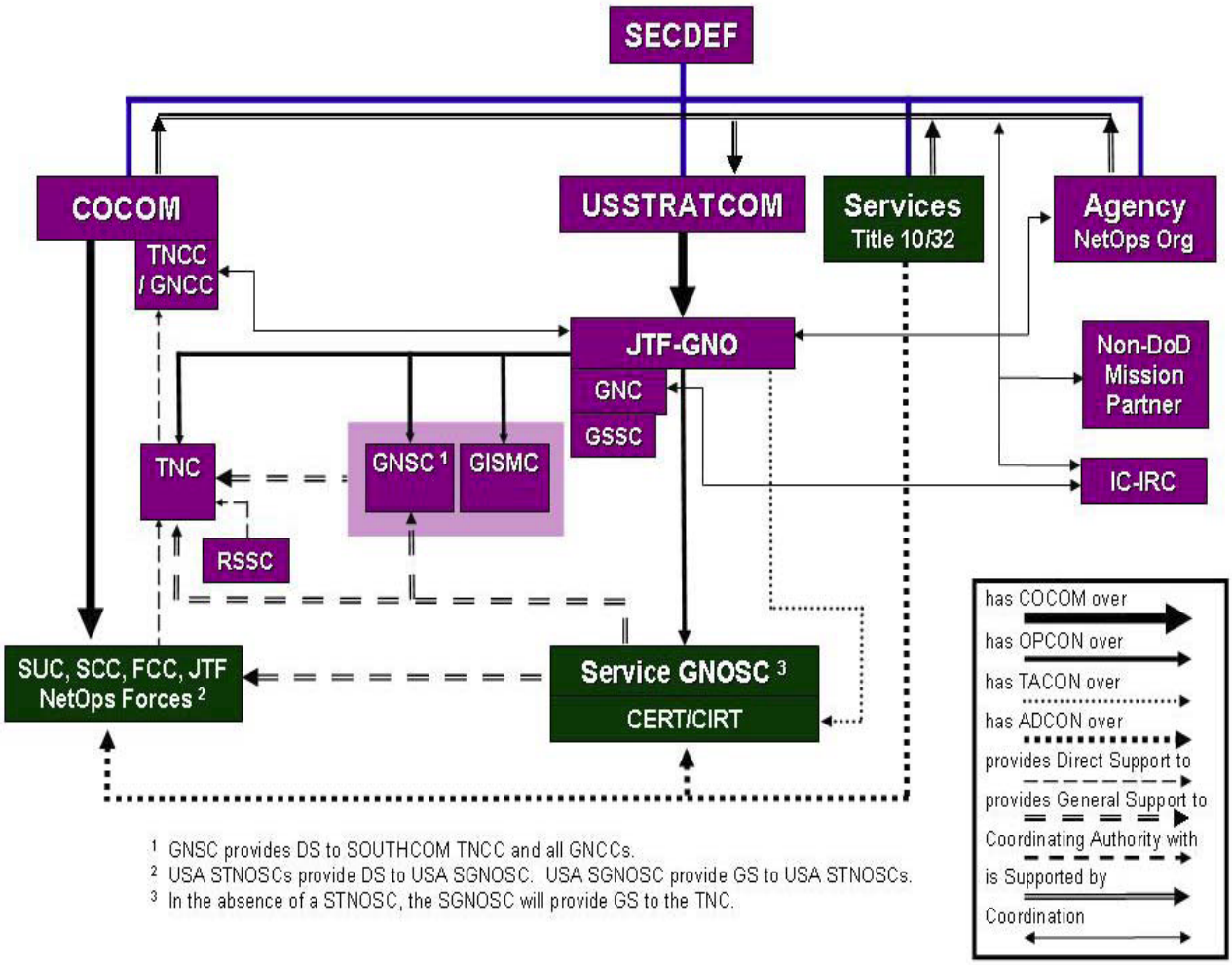

Figure 6 Global NetOps C2: USSTRATCOM is Supported Command

The independent primary researcher analysis also resulted in list of primary categorical Network Operations (NETOPS) themes of relevance. The primary researcher themes were not ranked, yet they were recorded as discoverable and prevalent across all strategic plans analyzed. The primary research NETOPS themes are presented in Table 2.

Themes
Net-Centricity – Modular/Decentralized/Collaborative
Data/Information Sharing – Speed to Decision
Acquisition – Technologies/Security/Training
Policy – Administrative/Operational
Doctrine – Joint/Inter-Service/Allied
Concepts of Operations (CONOPS)
Training – Enlisted/Officer/Civilian
Leadership – All levels/organizations
Administrative Chain of Command – Advisory/Strategic
Operational Chain of Command – Decisive
Enterprise Architecture – Interoperable/Capabilities & Effects Based

Table 2 Primary Researcher Themes

As can been seen, some of these initial themes can be consolidated due to cross-functionality and perspective interpretation of the particular entity authoring the strategic plan. Noting this possible perspective interpretation, the primary researcher consolidated the themes with relevance placed upon the perspective of the reader (the lowest common denominator). This resulted in a consolidated listing of themes, shown in Table 3.

Perspective Modified Themes
Net-Centric Data/Information Sharing – DIACAP, DISCAP, Net-Centric Policy, Data/Information, Acquisition Policy/guidance
Policy, Doctrine, CONOPs, Training – Joint/Allaince/Agency Publications/Policy/Training
Enterprise Architecture – GIG, DODIIS, LandWarNet, FORCEnet, C2 Constellation Net
Leadership, Chain of Command – CIO/COCOM/NETOPS Commander/Executive Collaboration Boards

Table 3 Primary Researcher Perspective Modification of Themes

Alternate Recorder/Coder Data

To provide rigor and validity to the primary researcher results an alternate recorder/coder was used to independently analyze the body of text. These coder results were collected to test the

content analysis framework and verify the results of the primary researcher. This rigor and validity also helps to solidify the reliability of the final results.

The alternate coder also independently coded all of the strategic plans in this body of text and recorded/coded the results within a Microsoft Excel spreadsheet (see Appendix B: "Sample Codebook"). The alternate recorder/coder was allotted 96 hours to conduct recording/coding on the body of text. The independent coding efforts were crucial to prevent invalidation of the data due to collaborative coding. The alternate recorder/coder did not have access to the primary researcher's recorded/coded data. The final codebook is a formulation of the annotations from the content analysis performed independently by the primary researcher and the alternate recorder/coder.

Due to the thematic nature of the recording/coding of the body of text, exact matches were not the goal. Holistic themes and idealistic agreements were the ultimate goal. The nature of strategic plans is not exact universal translation to each entity that views them. Rather, it is that internalization of the context that results in the implementation of the strategic plan based upon the perspective of the readers and the focus of the organization to which the reader is assigned. This being stated, the results of the alternate recorder/coder we interesting, to say the least.

The independent alternate recorder/coder analysis resulted in list of primary categorical Network Operations (NETOPS) entities, organizations, or levels within organizations of significance. The alternate recorder/coder categorical Network Operations (NETOPS) players were not ranked, yet they were tabulated based upon authorship and organizational responsibility for the content of the strategic plan. This resulted in the following table of primary categorical Network Operations (NETOPS) players.

Network Operations Players
Departmental – Chief Strategists
Chairmen of the Joint Chiefs of Staff – Authoritative Doctrine
Military Service Chief Information Officers – Inter/Intra Service Policy
Combatant Commander – Joint Tactics & Techniques
Military Service Commands – Operational/Tactical Direction
Intelligence (Agency & Service) – Information Technology/Systems/Policy
Inter/Intra Agency Organizations – Cross functional coordination
Multinational Entities – Global/Theater Coordination & Strategic Collaboration

Table 4 Alternate Recorder/Coder NETOPS Players

The alternate recorder/coder analysis also resulted in list of primary categorical Network Operations (NETOPS) themes of relevance. The alternate recorder/coder themes were not ranked, yet they were recorded as discoverable and prevalent across all strategic plans analyzed. The Alternate researcher NETOPS themes are presented in the Table 5.

Themes
Material – Technologies/Standardization
Education – Intrinsic Knowledge of Responsibilities
Personnel – Cadre of Special (IT/IM) Individuals/Digital Warriors
Facilities – Synchronized Capabilities/Critical Infrastructures
Doctrine – Practical/Formal/Persistent/Updated/Standard Taxonomy
Leadership – NETOPS/Critical Infrastructure/Enterprise Focused
Training – IT/IM/IA – Information Certification for All Levels
Organization – Synchronization/Standardization/Formulization

Table 5 Alternate Recorder/Coder Themes

As with the primary research themes, the alternate recorder/coder initial themes can be consolidated due to cross-functionality and perspective interpretation of the particular entities authoring the strategic plans. Noting this possible perspective interpretation, the primary researcher consolidated the themes with relevance placed upon the perspective of the reader (the

lowest common denominator). This resulted in a consolidated listing of the alternate recorder/coder themes, as shown in Table 6.

Perspective Modified Themes
Material & Facilities - Technologies/Standardization/Synchronized Capabilities/Critical Infrastructures
Leadership & Personnel - Cadre of Special (IT/IM) Individuals/Digital Warriors/ NETOPS/Critical Infrastructure/Enterprise Focused
Education & Training - Intrinsic Knowledge of Responsibilities/ IT/IM/IA – Information Certification for All Levels
Organization & Doctrine - Practical/Formal/Persistent/Updated/Standard Taxonomy/ Synchronization/Standardization/Formulization

Table 6 Alternate Recorder/Coder Perspective Modification of Themes

Combined Primary Researcher/Alternate Coder Data

The combined analysis of the primary researcher and the alternate recorder/coder resulted in two analytical constructs for visualizing the relationship of the discovered themes to NETOPS. As with the primary researcher and alternate recorder/coder themes tabulated in Table 3 and Table 6, respectively, the themes are not uniquely distinctive or separate. The themes tabulated by the primary researcher are correlated and interwoven, as can be seen in Figure 7.

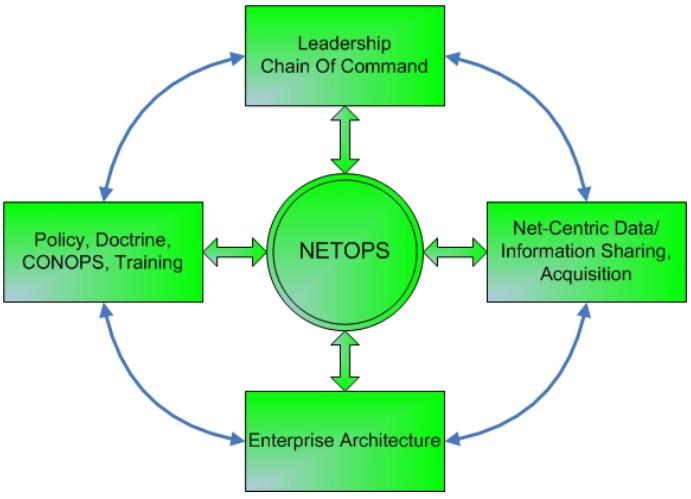

Figure 7 Primary ResearcherThematic Construct

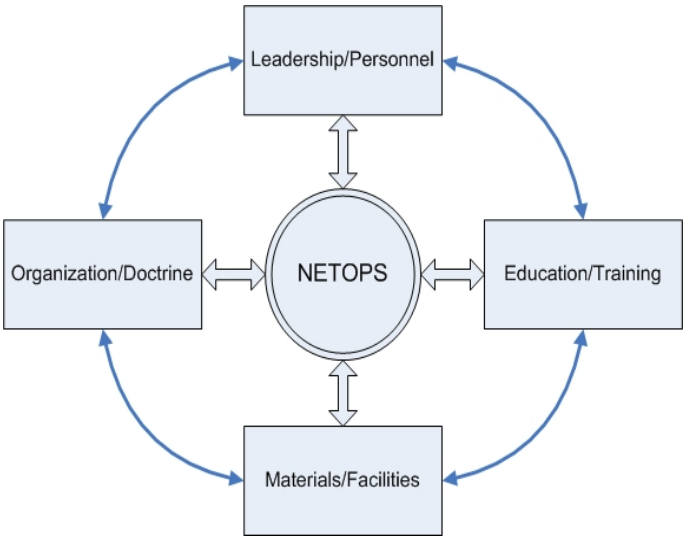

Figure 8 Alternate Recorder/Coder Thematic Construct

The themes tabulated by the alternate recorder/coder are correlated and interwoven, as can be seen in Figure 8. Using the discovered themes and the individual constructs that reflect the primary researcher and alternate recorder/coder interrelated themes to NETOPS, a combined construct can be envisioned. Figure 9 shows the primary researcher construct combined with the alternate recorder/coder construct (alternate construct detailed in red) to show an interwoven agreement and an alignment of themes. Figure 10 shows the alternate recorder/coder construct combined with the primary researcher construct (primary construct detailed in red) to show an interwoven agreement and an alignment of themes.

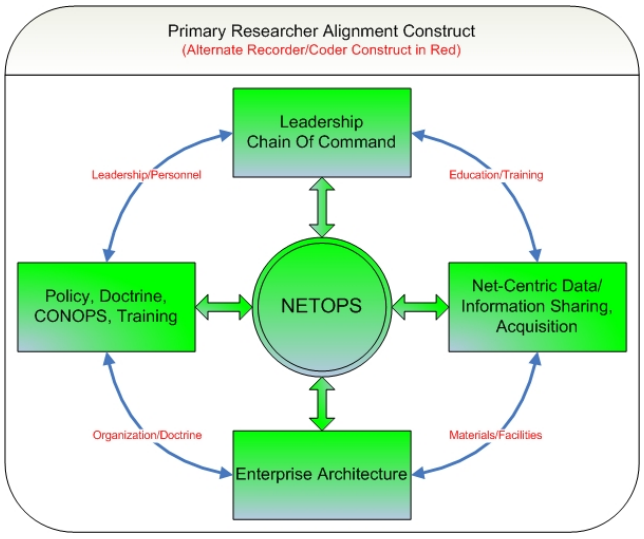

Figure 9 Primary w/Alternate Combined

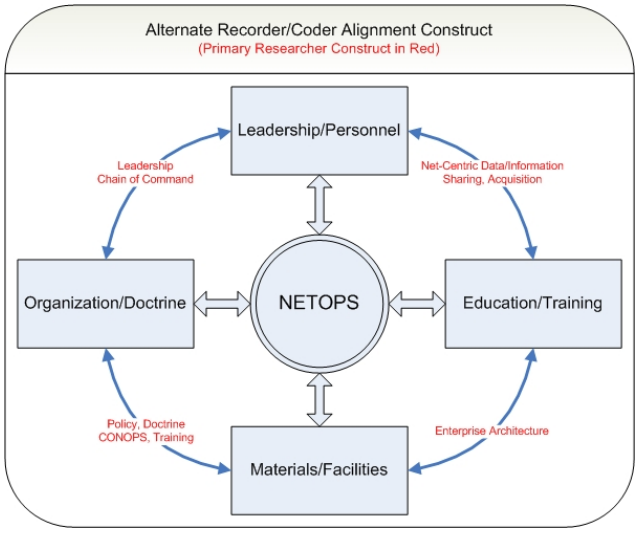

Figure 10 Alternate w/Primary Combined

The perspectives and discovered themes of the primary researcher and alternate recorder/coder constructs shown within Figure 9 and Figure 10 flow together thematically. The interwoven agreements of the themes to, within, and through NETOPS are evident.

In conducting the research both the primary researcher and the alternate recorder/coder discovered that internal and external guidance, respectively, played a major role in the

development of the strategic plans of the entities and organizations. For the primary researcher these internal guidance elements that were present were principle-like, not necessarily codified in policy or doctrine. The following quotes illustrate the guiding principles discovered by the primary researcher:

1. "Deploy interoperable, Joint IM and IT solutions to enhance warfighter effectiveness…align Department-wide IM and IT efforts with warfighter priorities…assure global secure access to information [and] lead continuous capability-enhanced IM and IT transformation...optimize information resources and investments, by maximizing return on investments, increasing efficiency, expanding the use of Enterprise solutions, and measuring the contribution of IT investments to warfighting effectiveness…adopt and share best practices" (DON, 2005b)
2. We are fleet/joint warfighter focused…connecting and protecting warfighters whenever, wherever…act with the utmost integrity...through integrity, our actions reflect our commitment to Navy's core values…we are agile and responsive...ensuring that our operations and solutions optimize responsiveness to the warfighter…adaptive...fostering an environment of continuous improvement, innovation and learning that makes NETWARCOM a great place to work…We are a team…focused on making FORCEnet a reality, enhancing every aspect of Naval, Joint, and combined operations" (NNWC, 2006a)
3. Recruit, train, and retain quality C4 Marines and Civilian Marines…ensure that our C4 training and education meet the needs of all our personnel who will employ and maintain tomorrow's C4 systems…GIG Enterprise Services and the foundation for enabling Network Centric Warfare (NCW) in the Marine Corps…field joint C4

systems that are secure, scalable, integrated, interoperable, modular, and reliable…exploit emerging technologies to provide increased capabilities…cultivate a closer bond between the Advocates…and the supporting C4 community….promote enterprise solutions that leverage best business practices and methods of operation" (HQMC/C4, 2004)

4. To operate cohesively as a single enterprise…to provide information that is accessible across the Intelligence Community (GDIP, 2006).

For the alternate recorder/coder theses external guidance elements that were present were codified in executive strategy, policy or doctrine. These quotes from the following executive strategy/policy/doctrine are indicative of the external guidance annotated by the alternate recorder/coder:

1. "Transform America's national security institutions to meet the challenges and opportunities of the twenty-first century" (POTUS, 2006a, p. 43).
2. "We will conduct network-centric operations with compatible information and communications systems, usable data, and flexible operational constructs…beyond battlefield applications, a network-centric force can increase efficiency and effectiveness across defense operations, intelligence functions, and business processes...a network-centric force requires fundamental changes in process, policy, and culture" (DOD, 2005c, p. 14).
3. "...creation of a collaborative information environment that facilitates information sharing, effective synergistic planning, and execution of simultaneous, overlapping

operations... on demand to defense policymakers, warfighters and support personnel" (CJCS, 2004, p. 25).

4. "We have set about making US forces more AGILE and more expeditionary" (DOD, 2006b, p. v).
5. Federal/Agency/Service Transformation Planning Guidance
6. Strategic Planning Guidance
7. Joint Operations Concepts Family

Both the primary researcher and the alternate recorder/coder stressed the importance of these external elements. The external elements guide not only the entity; they have a direct impact upon the entities' organizations and individuals within. This impact can influence the perspective, interpretation, and or the implementation of an entities strategic plan.

Answers to Research Questions

The results of this content analysis can be applied to answer the posited question: "Are the strategic plans of the organizations tasked with conducting NETOPS aligned?" The constructs developed from the discovered themes of the primary researcher and alternate recorder/coder directly answer the posited research question. There were internal and external elements discovered in the relationship of the themes annotated by the primary researcher and alternate recorder/coder, respectively. The extra element for the primary researcher was the guiding principles of the entities tasked with conducting NETOPS. The extra element for the alternate recorder/coder was the executive guidance that provided authoritative direction to the entities tasked with conducting NETOPS. The primary researcher and the alternate recorder/coder had 100% agreement that the strategic plans of the organization tasked with

conducting NETOPS are aligned. A developed construct containing the extra elements (executive guidance is detailed in **bold black** with guiding principles detailed in **bold blue**) in relation to the combined thematic constructs of the primary researcher and the alternate recorder/coder (alternate themes detailed in red) is shown in Figure 11. This construct illustrates the themes, as well as the internal and external influences, which show the alignment of the strategic plans of the organizations tasked with conducting NETOPS, are aligned. When the…elements of alignment are simultaneously connected, each element is supported and strengthened by the others…and great things happen" (Labovitz & Rosansky, 1997, p. 35/36).

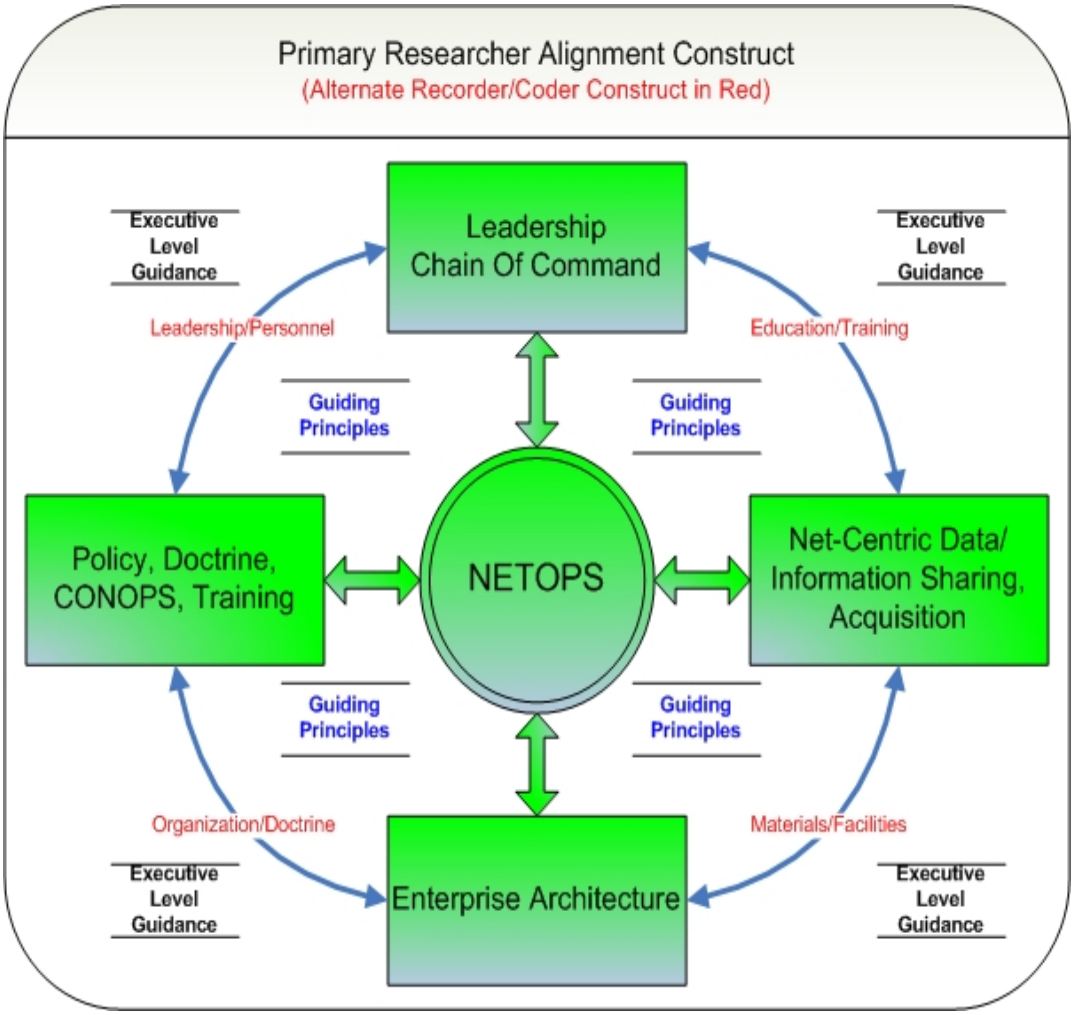

Figure 11 NETOPS Strategic Alignment Thematic Construct

This question was answered using a content analysis of the strategic plans of organizations that were tasked by federal policy, doctrine, or concepts of operations to conduct NETOPS. A Relevance Sampling of the body of text yielded 12 strategic plans for the organizations tasked with conducting NETOPS. The primary researcher and alternate recorder/coder analyzed the entire sample independently; resulting in the construct that represents the thematic NETOPS strategic plan alignment of the tasked organizations detailed in Figure 12.

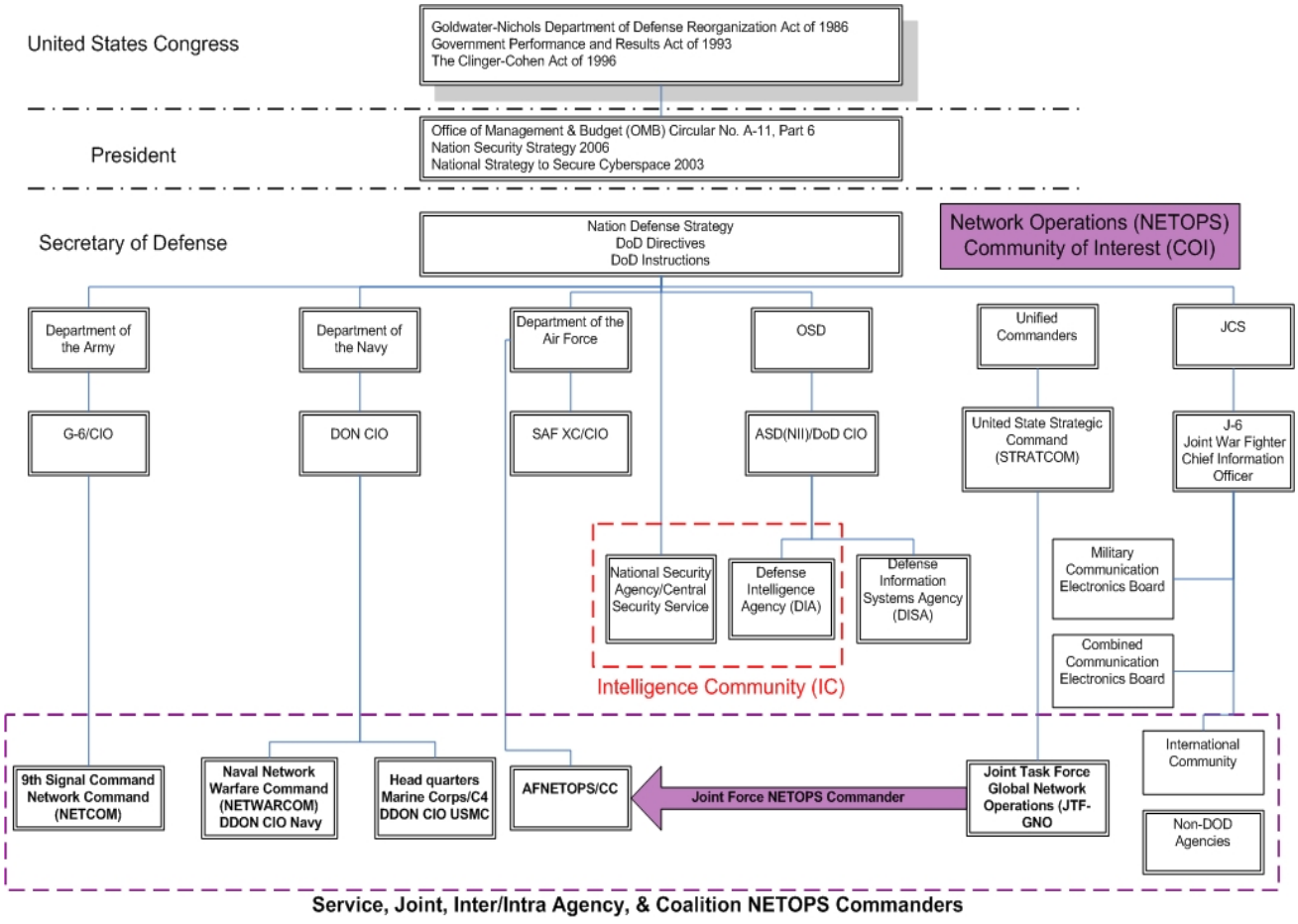

Figure 12 NETOPS Community of Interest Organization Chart

V. Discussion, Conclusions and Recommendations

Introduction

Joint, Inter/Intra Agency, and Allied/Coalition NETOPS strategic planning within and across organizations has become critical to conducting global network centric operations within the information domain of the global battle space. Within the Department of Defense global network environment, NETOPS strategic planning guides the implementation of network centric warfare focused directives. NETOPS Strategic planning incorporates and expands upon Global Information Grid policies and doctrine and ties them to the strategic goals and objectives of the NETOPS organization. NETOPS Strategic planning is used to develop, establish, and focus organizational policy, procedures, and processes for each organizations NETOPS responsibility with regard to their components of the GIG. These GIG components span the full range of business, intelligence, Warfighting, and defense operations. NETOPS Strategic planning specifically supports GIG overarching policy by defining near and long term goals, objectives, and as needed, roles and responsibilities for commands, services, and agency's foci on GIG NETOPS

Strategic plan alignment has been focused upon two distinct areas for organizations; establishing external competitive advantage, and internally aligning various aspects of an entity or organizations various components. Due to this focus, very little research has been done on the strategic alignment of multiple organizations with the same operational tasking at various levels within a globally dynamic area of operations.

Discussion

NETOPS is the central component/tenet of joint network mission-essential tasks (CJCS, 2006b, p. IV-1). When conducted with precision and effectiveness, "NETOPS provides integrated network visibility and end-to-end management of networks, global applications, and services across the [Global Information Grid]" (CJCS, 2006b, p. IV-1). As the importance of NETOPS continues to be defined by the policy, doctrine, and strategic elements of the Department of Defense, there are a few key issues that became evident during this research:

1. The NETOPS strategic environment is not as clearly defined at the tactical level of war as it is at the strategic and operational Levels of War (LoW).
2. Each command, service, agency has variable levels of importance placed upon the NETOPS mission; therefore cross communication occurs at multiple disjointed levels within the organizations.
3. There is still no consensus on the nature of the network as a weapons system within the Department of Defense.

Strategic to Tactical

The reality of NETOPS is that there are very few instances where a NETOPS even is not a globally impacting event. Global event and impact should be thought of as the norm, whereas theatre or regional events will be the exceptions to the rule. With the mindset that theatre and regional events are global in the aggregate, ASD/NII, the Joint Staff J-6, and STRATCOM must strategically define the operational and tactical organizational command and control relationships to conduct NETOPS. Joint Publication 0-2 espouses that "the keys to capturing and maintaining control over the battle rhythm

[is] simplicity" (CJCS, 2001a, p. xiv). This "simplicity" must include "unambiguous chain of command, well-defined command relationships, and clear delineation of responsibilities and authorities" (CJCS, 2001a, p. III-17). If "command is central to all military action, and unity of command is central to unity of effort" (CJCS, 2001a, p. x), then the global command and control relationships of the services and the joint environment (combatant command, etc) must have NETOPS strategic roles and responsibilities clearly defined at the tactical level of war beyond the scope of operational orders. Tactical entities need to be required to have strategic plans published and synchronized with their counterparts within and external to the combatant commanders, service, and agencies.

Joint from Disjointed

Within the NETOPS community of interest, it is evident that some organizations are functioning within their own realm of operations under completely different chains of command focused on the very same mission sets and objectives. This results in a fractured and extremely inefficient organizational structure within which to conduct NETOPS. As an example one service has a three-star (O-9) as the lead for conducting NETOPS, whereas another service has an O-6. With respect to most network-related activities and operations, the ability to task available resources to conduct NETOPS is not equal and results in a weakened NETOPS infrastructure. Some agencies, services, or commands do not have a centralized authority responsible for the collaborative and synergistic efforts to conduct NETOPS. This result is disjointed entities within the commands, service, and agencies with various level of responsibility for network Doctrine, Organization, Training, Materiel, Leadership, Education, Personnel, Facilities,

and Culture to scope the NETOPS environment. You can not build joint capabilities with disjointed, equally powerful, entities fielding NETOPS capabilities.

The Weapons System

The Department of Defense holistically does not manage networks as a weapons system. As net-centric operations and warfare has taken on an ever more importance as an enabler for information superiority and full spectrum dominance, DOD can not tactically afford to not develop the strategic capability to optimize interoperability, and therefore dependability of NETOPS assets. Managing network operations as a weapons system directs the appropriate level of focus on ensuring information assurance and network exploitation as an element of increased speed to decision and a force multiplier.

NETOPS strategic alignment is critical to successful operation of multiple layers of network centric warfare that can shift from decentralized, to centralized, then back to decentralize in a matter of seconds during multiple global engagements. To this researchers dismay, there are no models or construct examples for analyzing multiple organizations strategic plan alignment for the conducting of an over arching operation with multiple layers of cross-functionality, authority, and impact. Given the lack of previous accessible research in this area, the body of text analyzed in this research was used to form a foundation for future research. After a review of Joint architecture, network operations, national, defense, and military strategy, a posited research question was developed and answered in the affirmative as detailed in Chapter IV.

Research Limitations

There were a couple of limiting factors that can impact the results of this research effort. These limiting factors have been identified as researcher bias, recorder/coder training, and body of text selection.

Researcher Bias

There is no agreed upon "correct way" to analyze qualitative data (Leedy and Ormrod, 2005). Qualitative data interpretation tends to be more subjective in nature and may at times be influenced by the researcher's biases (Leedy and Ormrod, 2005). Effort was put into the data collection process to eliminate researcher bias due to background, previous knowledge, skills, and predisposition. To reduce researcher bias an alternate recorder/coder was used. This use of an alternate recorder/coder increases the collection of data and enhanced the different kinds of perspectives on the body of text being studied. The use of an alternate recorder/coder may even lead to contradicting information that may shed some light on the bias.

Recorder/Coder Training

With the exception of having the results of the primary researcher finding in validating the analytical framework, the alternate recorder/coder was trained using the exact same sample of material that the primary researcher used to validate the content analysis framework. An inter-recorder/coder agreement percentage of 100% would indicate that the recorder/coder training was successful. Yet, quantification of recorder/coder reliability is not a "defining criteria for content analysis" (Krippendorff,

2004, p. 87). There may be other factors that contributed to the high inter-recorder/coder percentage agreement.

Body of Text Selection

The researcher chose to use "Relevance Sampling" (Krippendorff, 2004, p. 119) for determining the body of text to be used within the content analysis. When the population for study is highly unique, it is feasible for the researcher to follow a conceptual (or considering context, a mandated) hierarchy, thereby reducing the number of textual units. Department of Defense Directives, Instructions, Doctrine and Concepts of Operations (CONOPS) that govern NETOPS were used as the definitive variables to determine the relevance of the sampled body of text for analysis. Krippendorff (2004) states that "Relevance Sampling selects relevant data in ways that statistical sampling theory has not yet addressed" (p. 120).

Yet, there are classified instruction, departmental, executive, service, and agency memorandums that are unattainable, that could have increased the relevant sampled or even the size of the body of text to be sampled from. All efforts were made to cross correlate the mandates of the available documents. Those mandates that were classified or inaccessible due to special access or "need to know" requirements will have to be used for future research at a possibly higher security classification level.

Suggestions for Further Study

This research effort was exploratory with the expectation that further research will be required to enhance the benefit f strategic planning within the NETOPS community. A follow-on research effort using the same methodological framework should be conducted

to further validate the findings and establish the reliability of the results and developed constructs. A follow-on research effort that delves into the other levels of strategic planning beyond the strategic and operational levels, for instance the tactical level, would provide a more holistic view of the NETOPS strategic alignment constructs developed in this research effort and validate its applicability.

A content analysis conducted by the Government Accountability Office (GAO) on the alignment of NETOPS organizations strategic plans would allow for a considerable amount of resources and expertise to be applied to the research that could not be mustered by this research effort. Given that theories espoused by the GAO were used in developing the criteria for alignment in this research, it is a matter or course that GAO should conduct a wider scale research effort beyond just the structure and content of a particular strategic plan (as is the nature of GAO content analysis in past research).

Summary

NETOPS is an organizational, procedural and technological construct for ensuring information superiority and enabling speed of command for the digital warrior. It links together widely dispersed network operations centers through a command and organizational relationship; establishes joint tactics, techniques and procedures to ensure a joint procedural construct; and establishes a technical framework in order to create a common network picture for the joint force commander (CJCS, 2006b).

Within the Joint Force Network Operations (NETOPS) environment, war fighters will treat net-centric adversaries and global information grid defense-in-depth situations as complex, adaptive enclaves that are the product of the dynamic interactions between

connected entities and processes. Because of net centricity, no entity or process of the enclave can be considered in isolation; no singular engagement methodology will accurately capture the enclave's complexity, and an alignment of Department of Defense Combatant Commanders, Services, and Agencies (CC/S/A) strategic planning is pivotal. To engage in this net-centric war fighting environment and achieve information dominance, the CC/S/A strategic plans must be structured, developed and delivered to meet the vision of the National Security Strategy, National Military Strategy, National Defense Strategy, and keystone documents for communications system support to NETOPS.

The goal of this research effort was to establish whether or not the strategic plans for organizations tasked with conducting NETOPS are aligned. Once the key organization were identified, their strategic plans could be analyzed used a structure content analysis framework. The themes discovered in the research effort, along with internal and external guiding elements, will hopefully lead to organizations successfully conducting NETOPS, and thereby achieving the results envisioned by the capabilities that NETOPS provides, enhances, and supports.

Appendix A – Strategic Plans used for Content Analysis

Air Force Communications Agency (AFCA). (2005). *Air Force Communications Agency Strategic Plan 2005-2015*. Scott Air Force Base, Ill: Author, 20 September 2005.

Chairman of the Joint Chiefs of Staff (CJCS). (2000). *Joint Vision 2020 - America's Military: Preparing for Tomorrow.* Washington, DC: Author, 24 May 2000.

Chairman of the Joint Chiefs of Staff (CJCS). (2004). *The National Military Strategy of the United States of America*. Washington, DC: Author, 18 March 2005.

Chairman of the Joint Chiefs of Staff (CJCS). (2005). *Capstone Concept for Joint Operations, Version 2.0.* Washington, DC: Director for Operational Plans and Joint Force Development, Joint Staff J-7 Joint Experimentation Transformation and Concepts Division.

Chairman of the Joint Chiefs of Staff (CJCS). (2006). *Joint Net-Centric Operations (JNO) Campaign Plan.* Washington, DC: Director for Command, Control, Communications, and Computer Systems Joint Staff J-6, 27 October 2006.

Chairman of the Joint Chiefs of Staff (CJCS). (2006). *Joint Publication 6-0, Communications System Support to Joint Operations.* Washington, DC: Director for Command, Control, Communications, and Computer Systems Joint Staff J-6.

Chairman of the Joint Chiefs of Staff (CJCS). (2006). *National Military Strategy for the Global War on Terrorism (GWOT).* Washington, DC: Author, 01 February 2006.

Chairman of the Joint Chiefs of Staff (CJCS). (2006). *National Military Strategy to Combat Weapons of Mass Destruction (WMD).* Washington, DC: Author, 13 February 2006.

Chief Information Officers Council (CIO). (2007). *Federal Chief Information Officers Council Strategic Plan FY 2007-2009*. Washington, DC: Federal Chief Information Officers Council, 22 January 2007.

Combined Communications-Electronics Board (CCEB). (2006). *Combined Communications-Electronics Board (CCEB) Strategic Plan Version P36.* n.p.: Author, 17 May 2006.

Defense Advanced Research Projects Agency (DARPA). (2005). *Defense Advanced Research Projects Agency (DARPA) Strategic Plan*. Washington, DC: Author, 07 February 2005.

Defense Information Systems Agency (DISA). (2006). *DISA Strategy Book - Surety, Reach, Speed*. Washington, DC: Author, 01 August 2006.

Defense Intelligence Agency. (2006). *Defense Intelligence Agency (DIA) Strategic Plan 2006-2011*. Washington, DC: Defense Intelligence Agency, 13 September 2005.

General Defense Intelligence Program (GDIP). (2006). *General Defense Intelligence Program Information Technology Strategic Plan Fiscal Years 2008–2013*. Washington, DC: Defense Intelligence Agency Directorate for Information Management and Chief Information Officer, 01 May 2006.

Head Quarters U.S. Marine Corps, Command Control, Communications, and Computers (HQMC/C4). (2004). *U.S. Marine Corps C4 Campaign Plan - Transforming Marine Corps C4*. Washington, DC: Author, 16 March 2004.

Joint Task Force for Global Network Operations (JTF-GNO). (2006). *Joint Task Force for Global Network Operations (JTF-GNO) Strategic Plan.* Washington, DC: Author, 07 August 2006.

National Security Agency/Central Security Service (NSA/CSS). (2006). *National Security Agency/Central Security Service Strategic Plan.* Retrieved on 23 December 2006 from http://www.nsa.gov/about/about00006.cfm.

Naval Network Warfare Command (NNWC). (2006). *Naval Network Warfare Command Strategic Plan 2006–2010…A Framework for Decision-making.* Washington, DC: Commander, Naval Network Warfare Command, 02 June 2006.

Office of Force Transformation (OFT). (2003). *Military Transformation: A Strategic Approach.* Washington, DC: Director, Force Transformation, Office of the Secretary of Defense, 23 November 2003.

Office of the President of the United States (POTUS). (2002). *National Strategy for Homeland Security 2002*. The White House. Washington, DC: Author, 17 July 2002.

Office of the President of the United States (POTUS). (2003). *National Strategy to Secure Cyberspace*. The White House. Washington, DC: Author, 14 February 2003.

Office of the President of the United States (POTUS). (2003). *National Strategy for the Physical Protection of Critical Infrastructure & Key Assests*. The White House. Washington, DC: Author, 05 February 2003.

Office of the President of the United States (POTUS). (2006). *National Security Strategy of the United States of America*. The White House. Washington, DC: Author, 20 March 2006.

Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. (n.d.). *Defense Procurement and Acquisition Policy Strategic Plan 2004-2011*. Retrieved 23 December 2006 from http://www.acq.osd.mil/dpap/about/strategy.htm.

Office of the Under Secretary of Defense for Personnel and Readiness (USD P&R). (2006). *Under Secretary of Defense for Personnel & Readiness Strategic Plan*. Washington, DC: Office of the Under Secretary of Defense for Personnel and Readiness, 08 April 2006.

U.S. Army Network Enterprise Technology Command/9th Army Signal Command (NETCOM/9thASC). (2006). *U.S. Army Network Enterprise Technology Command/9th Army Signal Command Campaign Plan*. Fort Huachuca, AZ: Author, 12 June 2006.

U.S. Department of Defense (DOD). (2004). *Department of Defense Information Assurance Strategic Plan v1.1 January, 2004*. Washington, DC: Defense-wide Information Assurance Program (DIAP), 27 January 2004.

U.S. Department of Defense (DOD). (2005). *The National Defense Strategy of the United States of America*. Washington, DC: Author, 18 March 2005.

U.S. Department of Defense (DOD). (2006). *2006 Department of Defense Chief Information Officer Strategic Plan Version 1*. Washington, DC: Author, 27 October 2006.

U.S. Department of Defense (DOD). (2006). *Quadrennial Defense Review Report*. Washington, DC: Author, 6 February 2006.

U.S. Department of Defense (DOD). (2006). *Strategic Plan for Department of Defense Training Transformation*. Washington, DC: Office of the Under Secretary of Defense for Personnel and Readiness Director, Readiness and Training Policy and Programs, 08 May 2006.

U.S. Department of Homeland Security (DHS). (2003). *Department of Homeland Security Strategic Plan 2004*. Washington, DC: Author, 23 February 2003.

U.S. Department of the Air Force (DOAF). (2005). *The U.S. Air Force Networking Operations (AFNETOPS) Transformation Flight Plan 2005*. n.p.: Office of Warfighting Integration and Chief Information Officer (SAF/XC), November 2005.

U.S. Department of the Army Chief Information Officer/G-6 (CIO/G-6). (2006). *U.S. Department of the Army Chief Information Officer/G-6 500 Day Plan Update 2005-2007*. Washington, DC: Author, October 2006.

U.S. Department of the Navy (DON). (2005). *Department of the Navy Information Management and Information Technology Strategic Plan FY 2006-2007*. Washington, DC: Department of the Navy Chief Information Officer (CIO), 02 November 2005

U.S. Strategic Command (STRATCOM). (2006). *Joint Concept of Operations for Global Information Grid Network Operations Version 3*. Offutt Air Force Base, Nebraska: Author, 04 August 2006.

Appendix B – Sample Codebook

(Part 1 of 2)

Author	NETWARCOM	HQMCC4	NETCOM/9th Signal	DISA	GDIP IT STRAT (IC)	CCEB
Document Title	Strategic Plan - A Framework for Decision Making	Command, Control, Communications and Computer (C4) Campaign Plan	NETCOM 9th Army Signal Command Campaign Plan	Defense Information Systems Agency Strategy Book - Surety, Reach, Speed	General Defense Intelligence Program Information Technology Strategic Plan	Combined Communications-Electronics Board (CCEB) Strategic Plan Version P36
Command/Service/Agency	Navy NETOPS	USMC NETOPS	Army NETOPS	Agency NETOPS	Agency NETOPS	Coalition NETOPS
Document Number	5	6	9	10	11	12
Release Date of Strategic Plan	June-06	May-04	June-06	July-06	April-06	May-06
Goal - 3	Ensure Navy fully leverages and influences Space capabilities. - Ensure no unnecessary redundancy of effort between other DoD Space communities and NETWARCOM's role as the Naval operational agent for Space.	Goal #3: Populate the Network - While the Marine Corps builds a secure common network, it needs to be populated with reliable, secure, and useful information. Together with MCCDC, MCWL, MCSC, and MCNOSC, HQMC C4 is determined to ensure that IT developments are synchronized from the ground up to facilitate network integration and interoperability across the MCEN.	• Conduct Network Operations within the Joint framework to enable assured information dominance and protected network-centric capabilities across the force.	• Operational excellence – accelerate operational effectiveness and efficiency. • NetOps • Automate the management and control of the network using machine-to-machine concepts and technology to reduce human intervention, improve availability and security, and reduce costs. • Develop a concept for leaner, more efficient NetOps presence to optimize performance and customer support and defend the network.	Goal 3 – IT Infrastructure: Achieve a global enterprise service delivery operating model	Goal 3: Champion actions to optimize Military access to spectrum. Provide the Warfighter with access to adequate radio frequency spectrum
Goal - 4	Develop the workforce to achieve information superiority. - Sustain, retain, attract, and develop a qualified/certified, diverse workforce to meet mission requirements as measured by ratings from recipient organizations, achieving ratings of "meet requirements" or "exceed requirements" for personnel within the information domain.	Goal #4: Protect the Network - The United States has the world's strongest military and largest economy. Both are increasingly reliant on critical infrastructures and on computer and telecommunications systems to support essential information capabilities. These information systems—vital to the Marine Corps' ability to carry out the DoD mission—are targets for our adversaries. We must therefore be able to safeguard the network from attack and preserve our ability to provide reliable and effective network services. The Commander US STRATCOM is the Combatant Commander for information operations, including global NetOps and CND missions, and as such is responsible for operation and defense of the GIG. The Marine Corps element of this global NetOps and CND strategy is the MCNOSC. In this role, the MCNOSC functions as a central element in protecting and preserving Marine Corps network services.	• Deliver interoperable global enterprise services and standards, while establishing Tactics, Techniques and Procedures in direct support of expeditionary forces.	• Sharing and defense of information – enables sharing of information while staunchly protecting it. - Defense in Depth - Develop and implement a defense-in-depth and detection-in-depth three-year DoD-wide plan across the DOTMLPF that meets the Department's mission assurance, secrecy, and sharing needs. - Acquire and support deployment of enterprise-wide tools and capabilities that improve defense, attack sensing and reaction, and situational awareness. - Develop compliance mechanisms in DoD processes to drive implementation of this plan (e.g. acquisition, certification and accreditation processes). • Develop a DoD-wide strategy for detection and deterrence of the insider threat.	Goal 4 – IT Management: Employ integrated IT investment management capabilities to enable standardized, objective decision making that promotes investments to achieve mission outcomes.	

Appendix B – Sample Codebook

(Part 2 of 2)

Author		NETWARCOM	HQMCC4	NETCOM/9th Signal	DISA	GDIP IT STRAT (IC)	CCEB
Document Title		Strategic Plan - A Framework for Decision Making	Command, Control, Communications and Computer (C4) Campaign Plan	NETCOM 9th Army Signal Command Campaign Plan	Defense Information Systems Agency Strategy Book - Surety, Reach, Speed	General Defense Intelligence Program Information Technology Strategic Plan	Combined Communications-Electronics Board (CCEB) Strategic Plan Version P36
Command/Service/Agency		Navy NETOPS	USMC NETOPS	Army NETOPS	Agency NETOPS	Agency NETOPS	Coalition NETOPS
Document Number		3	6	9	10	11	12
Release Date of Strategic Plan		June-06	May-04	June-06	July-06	April-06	May-06
Mission	Vision	NETWARCOM's superior information capabilities will drive joint force knowledge integration and implement network centric operations.	We will ensure the Marine Corps continues to be the world's most capable expeditionary fighting force by dramatically enhancing the expeditionary and joint C4 capabilities of the Marine Air Ground Task Force through the application of information technologies.	Trained professionals, strategically postured, transformed and ready for war, providing a joint network-centric information dominant enterprise to enable the Warfighter.	We are the provider of global net-centric solutions for the Nation's warfighters and all those who support them in the defense of the nation.	A centrally managed IT enterprise enabling the continually improving delivery of capabilities to the DoD intelligence enterprise.	CCEB enables C4 interoperability for member nations. Focus is on interoperability between member nations at the Strategic, Operational, and Tactical levels of command.
		To ensure our leaders have the information, mechanisms, and technology to make rapid and well-informed effects-based decisions, to degrade our enemies' decision capabilities, and to influence the decision-making of others in all phases of operations.	the c4 department is responsible for overseeing, planning, directing, and coordinating information technology (it) capabilities that support both the warfighting and business domains. the department influences the combat development process by establishing policies and standards for the marine corps enterprise architecture to foster joint and combined interoperability.	Execute globally based and expeditionary communications capabilities to enable joint and combined battle-command, leveraging the information grid to ensure extension and reach back capabilities to the Warfighter while operating, engineering, transforming and defending the Army's LandWarNet enterprise across the full spectrum of network-centric operations and warfare.	The Defense Information Systems Agency is a combat support agency responsible for planning, engineering, acquiring, fielding, and supporting global net-centric solutions to serve the needs of the President, Vice President, the Secretary of Defense, and other DoD Components, under all conditions of peace and war.	Embrace a centralized approach to managing the IT enterprise, utilizing best practices while advancing data sharing and information. GDIP's ability to support a transformed intelligence environment depends on the timeliness, quality, agility, and precision of the information provided.	CCEB has a mandate from member nations and other fora to provide leadership in the development of C4 capabilities within the combined and joint environment. Working to priorities agreed with member nations and other international fora, the CCEB seeks to achieve interoperability by developing and agreeing policies, procedures and standards. This is achieved by influencing national programmes to deliver capabilities for the exchange of all information in the combined or coalition environment.
Relationships		DOD, JTF-GNO, IC, NSA, DOTMLPF, USMC, STRATCOM	Defense Planning Guidance and the C4ISR transformational four-part strategy to Build, Populate, Protect, and Exploit the Network. GIG, C2 Constellation, LandWarNet, FORCEnet, Industry partners, C4 Campaign Plan - This C4 Campaign Plan serves as a roadmap for the C4 community as well as for our Marine Corps Advocates. Our future depends on an evolving capability that embraces joint and combined interoperability, emerging C4 technologies, expeditionary packaging, and the leadership of our "information warriors."	JTF-GNO, COCOMS	Services, Components, Agencies	DIA the Service Intelligence Centers, the unified combatant commands, the Defense Joint Intelligence Operations Center (DJIOC), the unified combatant command JIOCs, JIOC USFK, JIOC Iraq, and Reserve Intelligence Production Activities.	The member nations of the CCEB are Australia, Canada, New Zealand, the United Kingdom and the United States of America. Service fora, MIC, TTCP and NATO with regards to C4.
Focused Tasking		Y	Y	Y	N	N	N

References

67th Network Warfare Wing (67NWW). (2006). *Fact Sheet.* Retrieved on 18 November 2006 from http://www.8af.acc.af.mil/library/factsheets/factsheet.asp?id=4924.

Bean, William C., Domb, Ellen. (1993). *Strategic Planning That Makes Things Happen*. Amherst, Massachusetts: Human Resource Development Press, 1993.

Bryson, John M. (2004). *Strategic Planning for Public and Nonprofit Organizations: A Guide to Strengthening and Sustaining Organizational Achievement.* San Francisco, CA: Jossey-Bass Publishers, 2004.

Chairman of the Joint Chiefs of Staff (CJCS). (2001a). *Joint Publication 0-2, Unified Action Armed Forces (UNAAF).* Washington, DC: Commander, United States Joint Forces Command, Joint Warfighting Center Code JW100.

Chairman of the Joint Chiefs of Staff (CJCS). (2001b). *Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms (As Amended Through 9 November 2006).* Washington, DC: Director for Command, Control, Communications, and Computer Systems Joint Staff J-6.

Chairman of the Joint Chiefs of Staff (CJCS). (2003). *Defense Information System Network (DISN): Policy, Responsibilities, and Processes (Current as of 30 August 2006)*(CJCS Instruction 6211.02B). Washington, DC: Author, 31 July 2003.

Chairman of the Joint Chiefs of Staff (CJCS). (2004). *National Military Strategy of the United States of America - A Strategy for Today; A Vision for Tomorrow.* Washington, DC: Author, 18 March 2005.

Chairman of the Joint Chiefs of Staff (CJCS). (2005). *Capstone Concept for Joint Operations, Version 2.0.* Washington, DC: Director for Operational Plans and Joint Force Development, Joint Staff J-7 Joint Experimentation Transformation and Concepts Division.

Chairman of the Joint Chiefs of Staff (CJCS). (2006a). *Information Assurance (IA) and Computer Network Defense (CND)* (CJCS Manual 6510.01D, Change 3). Washington, DC: Author, 08 March 2006.

Chairman of the Joint Chiefs of Staff (CJCS). (2006b). *Joint Publication 6-0, Communications System Support to Joint Operations.* Washington, DC: Director for Command, Control, Communications, and Computer Systems Joint Staff J-6.

Chairman: functions (2006). Title 10 U.S. Code, Chapter 5 § 153 et seq. Retrieved 25 September 2006 from http://www.law.cornell.edu/uscode/html/uscode10/usc_sec_10_00000153----000-.html.

Chief Financial Officers Act of 1990 (CFO). 31 U.S.C. § 901 et seq.

Chief Information Officers Council (CIO). (2003). *Chief Information Officers Council Charter*. Washington, DC: Author, 05 December 2003.

Chief Information Officers Council (CIO). (2007). *Chief Information Officers Council MembershipListings*. Retrieved 25 January 2007 from http://www.cio.gov/index.cfm?function=memberlist.

Clinger-Cohen Act of 1996 (CCA). 44 U.S.C. § 3506 et seq.

Cresswell, J.W. (2003) *Research Design - Qualitative, Quantitative, and Mixed Methods Approaches*. Thousand Oaks, CA: Sage Publications, 2003

Denzin, N., & Lincoln, Y. (2000). *Topology of Qualitative Analysis Techniques, Handbook of Qualitative Research*. California: Sage Publications, 2000.

E-Government Act of 2002 (E-Gov). 44 U.S.C. § 3603 et seq.

General Defense Intelligence Program (GDIP). (2006). *General Defense Intelligence Program Information Technology Strategic Plan Fiscal Years 2008–2013*. Washington, DC: Defense Intelligence Agency Directorate for Information Management and Chief Information Officer, 01 May 2006.

Goldwater-Nichols Department of Defense Reorganization Act of 1986 (GNA). 10 U.S.C. § 164 et seq.

Government Performance and Results Act of 1993 (GPRA), 5 U.S.C. § 306 et seq.

Harvard Business Essentials. (2005). From Strategy to Implementation: Seeking alignment. In Collis D. J. (eds.), Strategy: Create and Implement the Best Strategy for Your Business (pp. 61-75 Series). Boston, MA: Harvard business School Press

Head Quarters U.S. Marine Corps, Command Control, Communications, and Computers (HQMC/C4). (2004). *U.S. Marine Corps C4 Campaign Plan - Transforming Marine Corps C4*. Washington, DC: Author, 16 March 2004.

Holsti, O.R. (1969). *Content Analysis for the Social Sciences and Humanities*. Reading, MA: Addison-Wesley, 1969.

Kaplan, Robert S., Norton, David P. (2006). *Alignment: Using the Balanced Scorecard to Create Corporate Synergies*. Boston, Massachusetts: Harvard Business School Press.

Krippendorff, K. (2004). *Content Analysis: An Introduction to Its Methodology* (2nd ed.). Thousand Oaks, CA: Sage, 1980.

Labovitz, G., Rosansky. (1997). The Power of Alignment. New York: John Wiley & Sons, Inc.

Leedy, P., and Ormrod, J. (2005) *Practical Research Planning and Design*. (8th ed.). Pearson Merrill Prentice Hall, 2005

Marine Corps Network Operations and Security Command (MCNOSC). (2006). *MCNOSC Homepage.* Retrieved on 23October 2006 from https://www.mcnosc.usmc.mil.

Naval Network Warfare Command (NNWC). (2006a). *Naval Network Warfare Command Strategic Plan 2006–2010…A Framework for Decision-making*. Washington, DC: Commander, Naval Network Warfare Command, 02 June 2006.

Naval Network Warfare Command (NNWC). (2006b). *Network Operations.* Retrieved on 23October 2006 from http://www.netwarcom.navy.mil.

Network Enterprise Technology Command (NETCOM). (2006). *The U.S. Army Network Enterprise Technology Command/9th Signal Command (Army).* Retrieved on 23October 2006 from http://www.netcom.army.mil/about/brochure/netcom.htm.

Neuendorf, K. (2002) *The Content Analysis Guidebook*. California: Sage Publications, 2002.

Office of Force Transformation (OFT). (2003). *Military Transformation: A Strategic Approach.* Washington, DC: Director, Force Transformation, Office of the Secretary of Defense, 23 November 2003.

Office of the President of the United States (POTUS). (1996). *Federal Information Technology* (Executive Order 13011). The White House. Washington, DC: Author, 16 July 1996.

Office of the President of the United States (POTUS). (2006a). *National Security Strategy of the United States of America*. The White House. Washington, DC: Author, 20 March 2006.

Office of the President of the United States (POTUS). (2006b). *Amendments to Executive Orders 11030, 13279, 13339, 13381, and 13389, and Revocation of Executive*

Order 13011 (Executive Order 13403). The White House. Washington, DC: Author, 12 May 2006.

Paperwork Reduction Act of 1995 (PRA). 44 U.S.C. § 3501 et seq.

Shea, R. M. (2006). The Team: Creating the Enabling Capability to Conduct Net-Centric Operations. *Crosstalk: The Journal of Defense Software Engineering, 19(7),* 18-20.

U.S. Air Force Office of Warfighting Integration and Chief Information Officer (SAF/XC). (2003). *Warfighting Integration: Winning the Global War on Terror* (SAF/XC Mission Brief). Retrieved 30 November 2006 from https://www.my.af.mil.

U.S. Department of Defense (DOD). (2002). *Management of DOD Information Resources and Information Technology* (DOD Directive 8000.1). Washington, DC: Assistant Secretary of Defense for Command, Control, Communications, and Intelligence/Chief Information Officer (ASDC3I/CIO), 20 March, 2002.

U.S. Department of Defense (DOD). (2003). Assistant Secretary of Defense for Command, Control, Communications, and Intelligence/Chief Information Officer (ASDC3I/CIO). *Global Information Grid (GIG) Overarching Policy* (DOD Directive 8100.1). Washington. DC: Author, 19 September 2002, Certified Current as of 21 November 2003.

U.S. Department of Defense (DOD). (2005a). *Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer (ASD(NII)/DOD CIO)*(DOD Directive 5144.1) . Washington, DC: Director of Administration and Management (DA&M), 02 May, 2005.

U.S. Department of Defense (DOD). (2005b). *Designation of the Director, Defense Information Systems Agency (DISA), as Commander, Joint Task Force – Global Network Operations (JTF-GNO)* (Secretary of Defense Memorandum). Washington, DC: Author, 17 November 2005.

U.S. Department of Defense (DOD). (2005c). *National Defense Strategy of the United States of America*. Washington, DC: Author, 18 March 2005.

U.S. Department of Defense (DOD). (2006a). *Defense Information Systems Agency (DISA)*(DOD Directive 5105.19) . Washington, DC: Director of Administration and Management (DA&M), 25 July, 2006.

U.S. Department of Defense (DOD). (2006b). *Quadrennial Defense Review Report*. Washington, DC: Author, 6 February 2006.

U.S. Department of Defense Chief Information Officer (DODCIO). (2001). *Department of Defense Global Information Grid Computing* (Guidance and Policy Memorandum 11-8450). Washington, DC: Author, 06 April 2001.

U.S. Department of the Air Force (USAF). (2006). *Information Resource Management* (Air Force Policy Directive 33-1). Washington, DC: Secretary of the Air Force, 27 June 2006.

U.S. Department of the Army (Army). (2005). *Army Knowledge Management and Information Technology Management* (Army Regulation 25-1). Washington, DC: Secretary of the Army, 15 July, 2005.

U.S. Department of the Navy (DON). (2003). *Designation of the Department Of The Navy Deputy Chief Information Officer (Navy) And Department Of The Navy Deputy Chief Information Officer (Marine Corps)* (Secretary of the Navy Memorandum). Washington, DC: Secretary of the Navy, 04 November 2003.

U.S. Department of the Navy (DON). (2005a). *Assignment of Responsibilities and Authorities in the Office of the Secretary of the Secretary of the Navy* (Secretary of the Navy Instruction 5430.7N). Washington, DC: Secretary of the Navy, 09 June 2005.

U.S. Department of the Navy (DON). (2005b). *Department of the Navy Information Management and Information Technology Strategic Plan FY 2006-2007*. Washington, DC: Department of the Navy Chief Information Officer (CIO), 02 November 2005

U.S. Department of the Navy (DON). (2006). *Designation of the Department of the Navy Deputy Chief Information Officer (Navy)* (Secretary of the Navy Memorandum). Washington, DC: Secretary of the Navy, 21 November 2006.

U.S. Government Accountability Office (GAO). (1998). *Managing for Results: Observations on Agencies' Strategic Plans* (GAO/T-GGD-98-66). Washington DC: U.S. Government Printing Office.

U.S. Government Accountability Office (GAO). (1999). *Using the Results Act and Quality Management to Improve Federal Performance* (GAO/T-GGD-99-151). Washington DC: U.S. Government Printing Office.

U.S. Office of Management and Budget (OMB). (2000). *Management of Federal Information Resources* (OMB Circular A-130). Washington, DC: Office of Management and Budget, 2000.

U.S. Office of Management and Budget (OMB). (2006). *Preparation and Submission of Strategic Plans, Annual Performance Plans, and Program Performance Reports*.

Part 6 to OMB Circular A-11, Preparation, Submission, and Execution of the Budget. Washington, DC: Government Printing Office, 2006.

U.S. Strategic Command (STRATCOM). (2006). *Joint Concept of Operations for Global Information Grid Network Operations Version 3*. Offutt Air Force Base, Nebraska: Author, 04 August 2006.

Vita

LT Antonio Scurlock was born in Chapel Hill, NC, graduated high school in 1987 then enlisted in the Navy May of 1991. He was attached to two Air Craft Carriers for avionics maintenance support. During these afloat operations from 1993 through 1995, he was assigned onboard USS NIMITZ (CVN-68) and the USS GEORGE WASHINGTON (CVN-73).

Selected for the Enlisted Commissioning Program (ECP) in 1995, he reported to the NROTC Unit at North Carolina State University (NCSU). In June 1997, he earned his Bachelor's degree in Political Science and was commission as an Ensign.

Shortly after receiving his commission, he served again onboard the USS NIMITZ (CVN-68) as the Y2K Assessment and Remediation Officer. He also served as an Aerospace Maintenance Duty Officer (AMDO) onboard the USS CARL VINSON (CVN-70) during Operation Enduring Freedom.

When the Navy created a special community of Information Professionals to manage its Information Technology, Information Systems and Enterprise Architecture, LT Scurlock was selected and transferred to Naval Network and Space Operations Command. Assigned as the Navy/Marine Corps Intranet (NMCI) Enterprise Training Officer, he was responsible for developing NETOPS Technicians to support the United States Navy components of the Global Information Grid (GIG).

In September 2005, LT Scurlock entered the Graduate School of Engineering and Management at the Air Force Institute of Technology as a participant in the Department of Defense (DOD) Information Assurance Scholarship Program (IASP).

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
22-03-2007	**Master's Thesis**	Aug 2005 – Mar 2007

4. TITLE AND SUBTITLE

Strategic Planning to Conduct Joint Force Network Operations: A Content Analysis of NETOPS Organizations Strategic Plans

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Scurlock, Antonio J., Lieutenant, USN

5d. PROJECT NUMBER
If funded, enter ENR #

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GIR/ENV/07-M18

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Office of Department of the Navy Chief Information Officer (DONCIO)
Attn: Ms. Sandra Smith
1000 Navy Pentagon
Washington, DC 20350-1000 Com: (703) 602-6545/(703) 601-0605

10. SPONSOR/MONITOR'S ACRONYM(S)
DONCIO

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

12. DISTRIBUTION/AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Within the Joint Force Network Operations (NETOPS) environment, war fighters will treat net-centric adversaries and global information grid defense-in-depth situations as complex, adaptive enclaves that are the product of the dynamic interactions between connected entities and processes. Because of net centricity, no entity or process of the enclave can be considered in isolation; no singular engagement methodology will accurately capture the enclave's complexity, and an alignment of Department of Defense combatant commanders, services, and agencies (CC/S/A) strategic planning is pivotal.

To achieve and maintain information dominance, Joint Network Operations (NETOPS) organizations need to be strategically aligned. Strategic alignment allows organizations tasked with conducting NETOPS to meet the needs of the NETOPS Combatant Commander, United States Strategic Command (USSTRATCOM) and as a result, to enhance the capabilities-based effects of NETOPS and reduce our NETOP infrastructures susceptibility to compromise.

The goal of this research effort was to answer the question "Are the strategic plans of the organizations tasked with conducting NETOPS aligned?" Once the key organizations were identified, their strategic plans were analyzed using a structured content analysis framework. The results illustrated that the organizations strategic plans were aligned with the community of interests tasking to conduct NETOPS. Further research is required into the strategic alignment beyond the strategic (national/theater) and operational levels to determine if the developed NETOPS strategic alignment construct is applicable to all level of war.

15. SUBJECT TERMS
Strategic alignment, Strategy, Strategic planning, NETOP, Joint Network Operations, Network operations, Information Technology, Information Management, Information resource management, Organizational Structure, Information Dominance, Content Analysis, IM, IT, IRM

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
REPORT	**ABSTRACT**	**c. THIS PAGE**			Dr. Alan Heminger, PhD
U	**U**	**U**	**UU**	84	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-3636, ext 7405; e-mail: alan.heminger@afit.edu

Standard Form 298 (Rev: 8-98)
Prescribed by ANSI Std. Z39-18