NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

LATERAL COORDINATION OF INTERDEPENDENT U.S. ARMY INFORMATION TASKS

by

Bren Workman

December 2008

Thesis Co-Advisors: Hy Rothstein
Erik Jansen

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2008	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Lateral Coordination of Interdependent U.S. Army Information Tasks		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Bren Workman			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

The purpose of this thesis is to determine whether the U.S. Army is adequately prepared or organizationally structured at the operational and tactical levels of warfare and command to execute synchronous information operations in light of recent doctrinal changes. Implementation of the new Army Field Manual (FM) 3-0, Operations, will significantly affect the conduct of information and influence operations in the U.S. Army at the operational and tactical levels of warfare and command. Field Manual 3-0, published February 27, 2008, revised how the Army views information operations and the staff responsibility for the tasks associated with them. U.S. Army information operations is now doctrinally divided into five Army information tasks, with the responsibility redistributed to different staff functional cells, ultimately to be synchronized by the operations process. The five Army information functional cells possess a reciprocal interdependence with each other, each providing inputs and feedback to the others. This study concludes that a lateral coordination process should be applied to the functional structure of the staff organization to accomplish information tasks. A direct liaison or full-time integrator role should be applied to the organization to integrate IO elements' capabilities and related activities and in order to synchronize information activities. The combined performance and effectiveness of the staff organization requires a lateral process of coordination to synchronize the highly-interdependent information tasks.

14. SUBJECT TERMS Information Operations, Information Superiority, Organizational Design, Task Interdependence, Lateral Coordination Processes			**15. NUMBER OF PAGES** 111
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

LATERAL COORDINATION OF INTERDEPENDENT U.S. ARMY INFORMATION TASKS

Bren K. Workman
Major, United States Army
Bachelor of Science, Kansas State University, 1994

Submitted in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE IN INFORMATION OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
December 2008

Author: Bren Workman

Approved by: Dr. Hy Rothstein
Thesis Co-Advisor

Dr. Erik Jansen
Thesis Co-Advisor

Dr. Gordon McCormick
Chairman, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The purpose of this thesis is to determine whether the U.S. Army is adequately prepared or organizationally structured at the operational and tactical levels of warfare and command to execute synchronous information operations in light of recent doctrinal changes. Implementation of the new Army Field Manual (FM) 3-0, *Operations*, will significantly affect the conduct of information and influence operations in the U.S. Army at the operational and tactical levels of warfare and command. Field Manual 3-0, published February 27, 2008, revised how the Army views information operations and the staff responsibility for the tasks associated with them. U.S. Army information operations is now doctrinally divided into five Army information tasks, with the responsibility redistributed to different staff functional cells, ultimately to be synchronized by the operations process. The five Army information functional cells possess a *reciprocal interdependence* with each other, each providing inputs and feedback to the others. This study concludes that a *lateral coordination process* should be applied to the functional structure of the staff organization to accomplish information tasks. A direct liaison or full-time integrator role should be applied to the organization to integrate IO elements' capabilities and related activities and in order to synchronize information activities. The combined performance and effectiveness of the staff organization requires a lateral process of coordination to synchronize the highly-interdependent information tasks.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I am grateful for the support of all who have generously assisted me with the research and writing of this thesis. Dr. Hy Rothstein and Dr. Erik Jansen have taken considerable time out of their busy schedules to help me devise a qualitative analysis of emerging Army doctrine. These personal and professional mentors have provided me with information and expertise from their vast accumulation of experience.

To my family: Lynne’, Brandy and Alex, who supported me during the countless hours of research and doctrinal analysis required for this project, my heartfelt appreciation goes out to you for your unwavering assistance, patience, understanding, and support. Thank you.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

C4OPS	Command, control, communications, and computer operations
CI	Counterintelligence
CNA	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Exploitation
CNO	Computer Network Operations
COA	Course of Action
COIN	Counterinsurgency
COMCAM	Combat Camera
CoS	Chief of Staff
DoD	Department of Defense
DSPD	Defense Support to Public Diplomacy
EA	Electronic Attack
EP	Electronic Protect
ES	Electronic Warfare Support
EW	Electronic Warfare
FA30	Functional Area 30 Information Operations Officer
FM	Field Manual
G/S-2	Intelligence Officer
G/S-5	Plans Officer
G/S-6	Communications Officer
G/S-7	Information Operations Officer
G/S-9	Civil Affairs Officer
IA	Information Assurance
IE	Information Engagement
IO	Information Operations
IPB	Intelligence Preparation of the Battlefield
IS	Information Superiority

J-39	Joint Information Operations Cell/Chief
JP	Joint Publication
JPG	Joint Planning Group
JTF	Joint Task Force
MILDEC	Military Deception
MDMP	Military Decision Making Process
NATO	North Atlantic Treaty Organization
OIF	Operation Iraqi Freedom
OPORD	Operation Order
OPLAN	Operation Plan
OPSEC	Operations Security
PA	Public Affairs
PSYOP	Psychological Operations
SC	Strategic Communication
WARNO	Warning Order

I. INTRODUCTION

A. BACKGROUND - THESIS OVERVIEW

Advances in information technology have changed the way U.S. Army forces operate, just as it continues to change every aspect of our society. The impact and importance of the information dimension of Army operations will likely continue to increase given a continuance of the current operational landscape characterized by persistent global conflict and complex, decentralized threats.

The Information Operations (IO) concept as envisioned by Army Field Manual (FM) 3-0, *Operations*, 2001, and codified by FM 3-13, *Information Operations: Doctrine, Tactics, Techniques and Procedures*, 2003, synchronized several previously disparate information capabilities and related activities for the purpose of achieving and maintaining *information superiority.*

While the 2001 version of FM 3-0 added information as an element of combat power, thus elevating the impact of the information dimension on the operational environment[1], the

[1] Joint Chiefs of Staff, *Joint Publication 3-0, Joint Operations,* 17 September 2006, Change 1, 13 February 2008, (Washington, D.C.: Joint Staff, 2006), p. GL-22, http://www.dtic.mil/doctrine/jel/new_pubs/jp3_0.pdf (accessed 2/24/08). Operational environments are a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. While they include all enemy, adversary, friendly, and neutral systems across the spectrum of conflict, they also include an understanding of the physical environment, the state of governance, technology, local resources, and the culture of the local population.

2008 FM 3-0 revises how the Army views information operations and the staff responsibility for the tasks associated with them.

CORE CAPABILITIES	
Electronic Warfare	Military Deception
Computer Network Operations	Psychological Operations
Operations Security	
SUPPORTING CAPABILITIES	**RELATED CAPABILITIES**
Information Assurance	Public Affairs
Physical Security	Civil-Military Operations
Counterintelligence	Defense Support to Public Diplomacy
Physical Attack	
Combat Camera	
DoD Information Operations: "The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision-making, while protecting our own."	

Figure 1. Joint Information Operations.[2]

Implementation of the new FM 3-0, *Operations*, published February 27, 2008, will significantly affect the conduct of information and influence operations in the U.S. Army operationally and tactically. As Army Capstone Doctrine, the 2008 FM 3-0 supersedes all subordinate operations doctrine, to include 'information operations,' doctrine.[3]

Field Manual 3-0, 2008 has dictated that the former 2003 concept of 'information operations' now be divided into five Army 'information tasks,' in regard to the work

---

[2] Joint Chiefs of Staff, *Joint Publication 3-13, Information Operations,* 13 February 2006, (Washington, D.C.: Joint Staff, 2006), p. ix, http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf (accessed 3/6/08). Various definitions of *Information Operations* exist between previous and current Joint and Army doctrine. For the purpose of this thesis, the Joint definition will be used which has been adopted by the Army and supersedes the Army's previous definition in the current-standing FM 3-13, *Information Operations*, and further includes the Related Capability of Defense Support to Public Diplomacy as recognized in the new FM, 3-0, *Operations*.

[3] U.S. Army doctrine hierarchy is described in Chapter II.

required to operate within the information dimension of the operational environment. The responsibility for executing these information tasks has been distributed to independent staff functional cells, to be ultimately synchronized through the operations process.

Task	*Information Engagement*	*Command and Control Warfare*	*Information Protection*	*Operations Security*	*Military Deception*
Intended Effects	Inform and educate internal and external publics Influence the behavior of target audiences	Degrade, disrupt, destroy, and exploit enemy command and control	Protect friendly computer networks and communi-cation means	Deny vital intelligence on friendly forces to hostile collection	Confuse enemy decision makers
Capabilities	Leader and Soldier engagement Public affairs Psychological operations Combat camera Strategic Communication and Defense Support to Public Diplomacy	Physical attack Electronic attack Electronic warfare support Computer network attack Computer network exploitation	Information assurance Computer network defense Electronic protection	Operations security Physical security Counter-intelligence	Military deception
Staff Responsibility	G-7 with PA, PSYOP and G-9 support within the information engagement cell	G-3 with G-2 support within the fires cell	G-6 within the Network Operations Cell	G-3; with G-2 support within the protection cell	G-5; within the plans cell

Key:
G-2 Intelligence – Responsible for the production and dissemination of combat intelligence and counterintelligence matters.
G-3 Operations and Training – Responsible for planning the successive military operations, organization, and training.
G-5 Plans – Responsible for the planning of future military operations and organization.
G-6 Communications – Responsible for Command, control, communications, and computer operations.
G-7 Information Operations – Responsible for employment of the core, specified and related capabilities of IO in support of achieving Information Superiority.
G-9 Civil Military Operations – Responsible for establishing, maintaining and influencing relations between military forces and the civilian populace.
PSYOP Psychological Operations – Responsible for informing foreign audiences to influence their emotions in order to affect desired behavior.
PA Public Affairs – Responsible for timely and accurate information dissemination to domestic and foreign audiences.

Figure 2. Army Information Tasks.[4]

[4] The 2008 FM 3-0 delineates five Army Information Tasks to leverage the power of information in full spectrum operations.

The figure above aligns staff responsibilities for accomplishing and synchronizing the five Army information tasks. This alignment has been a matter of considerable discussion and debate. The highlighted 'Staff Responsibility' row, though approved by General Schoomaker and General Casey in their position as Army Chief of Staff in January 2007 and February 2008, respectively, was not included in the 2008 FM 3-0. It was decided that Information Tasks responsibility should be addressed at lower-level doctrine, presumably in the pending FM 5-0, *The Operations Process*, or a future FM 3-13, *Information*, rather than in FM 3-0, the Army's capstone operations doctrine.

In *Organization in Action*, James D. Thompson describes three types of interdependence: *pooled interdependence*, where subtasks are performed separately and in any order; *sequential interdependence*, where subtasks are completed in a specified sequence; and, *reciprocal interdependence*, the highest form of interdependence, where the output of one coordination cell becomes the input for others.[5] The combined performance and effectiveness of a staff 'organization' operating in the information dimension may require a lateral process of coordination to synchronize the highly-interdependent information tasks.

Each of the five Army information tasks possess an inherent *reciprocal interdependence* to the other tasks as they cumulatively shape the information dimension of the operational environment. Specifically, in the execution of an information campaign in a theater of operations, the

[5] James D. Thompson, *Organizations in Action: Social Science Bases of Administrative Theory* (New York: McGraw-Hill, 1967), pp. 45-55, 52-53, 55-56.

output of one staff functional cell responsible for one information task could likely become the input to another cell accountable for another information task. This task interdependence that exists between the functional coordination cells' work requires effective coordination and problem solving. In turn, cross-unit coordination can be effectively achieved through lateral relationships or coordination mechanisms.[6]

To achieve the effectiveness of the staff to positively affect the information dimension of the operational environment, the Army can organize operational and tactical staffs by the designs dictated in recent doctrine:

1. FM 3-0, *Operations*, 2008

The U.S. Army's new capstone Operations doctrine asserts that all operations should be conceived in terms of affecting the human will and decision making as their ultimate purpose. The field manual invokes the supremacy of the moral dimension in conflict and the imperative to consider all operational aspects of the environment as a unity from inception through conclusion. Capitalizing on this unity begins with identifying those cognitive effects likely to produce the desired end state, and then designing an operation with physical actions, words, and images synchronized to best advance the desired outcomes. In this design, commanders are directly responsible for informational and cognitive effects as such effects are the cornerstone of their battle command. In accordance with

[6] Jay R. Galbraith, *Designing Complex Organizations* (Reading, Mass.: Addison-Wesley Pub. Co, 1973).

FM 3-0, 2008, the responsibility for coordinating the five Army information tasks and their corresponding capabilities rests with the staff principals operating in the functional coordination cells. The responsibility of the G/S-7 Information Operations Officer, is not to laterally coordinate all of the IO capabilities, but is limited to synchronizing information engagement activities as the staff lead for Army Information Task 1, Information Engagement, in concert with all other operational activities.

The responsibility for laterally coordinating the designated five Army information tasks and their corresponding capabilities are to be assigned to the accountable staff principals who already possess like capabilities, capacity, and knowledge in the organization. This design assumes that the staff principals use their corresponding functional coordinating cells to integrate these highly-interdependent information activities, and then relies on the operations process to laterally coordinate the activities between functional cells and into plans, orders, and synchronous military operations.

2. FM 3-0, *Operations*, 2001, and FM 3-13, *Information Operations*, 2003

The previous concept of the Information Environment as found in the 2001 FM 3-0 asserts there is a qualitative and categorical difference between combat operations and “information operations,” at least as far as staff proponent tasks are concerned. It contends that operations are focused on operational objectives, which may or may not be “cognitive.” The role of the Information Operations Officer in this design is to estimate the required information tasks

associated with the operational environment and develop courses of action with the IO capabilities that the commander would incorporate to achieve his objectives. In other words, the G/S-7 is the accountable staff principal who synchronizes information activities derived from his training, knowledge, and expertise of the full range of IO capabilities and related activities.

Some military information professionals who supported the organizational design of the 2001 FM 3-0 during the Information and Cyberspace Symposium[7] acknowledged that the older approach is not the most advantageous, but believe some form of lateral control should be retained, nonetheless, until the Army develops an intrinsic understanding of the power of information and the competency to apply that power as instinctively as it does fires and maneuver.

The two doctrinal concepts reflect two different ways of thinking and understanding the role of information in the contemporary operational environment and the integrating mechanisms necessary to synchronize required information tasks. The new FM 3-0 has directed the Army towards a command-centric view requiring the contribution of the entire team to achieve the potential of information as a unity with all operational activity in full spectrum operations. The challenge is that the 2001 FM 3-0 design is

[7] The U.S. Army Combined Arms Center hosted the Information and Cyberspace Symposium at Fort Leavenworth, Kansas, 15–18 April 2008. The symposium was attended by the author of this thesis and 135 other information practitioners and leaders from the national security community. A series of plenary sessions and workshops were used to determine, among other initiatives, the way ahead for publishing the necessary update to FM 3-13, *Information*, given the changes regarding information tasks in the newly-published FM 3-0, *Operations*.

rather common in current practice particularly at the operational and tactical levels of Army warfare and command.

The two organizational designs offer two ways in which to synchronize information activities with other operational activities and to integrate the result into the operations process. However, the two designs should not be considered contradictory. As this research asserts, it is important to integrate words and deeds than to integrate the employment of IO capabilities into one line of operation, yet, the combined performance and effectiveness of the staff organization' may require a simple or complex form of lateral coordination to synchronize the *reciprocal interdependent* information tasks. The operations process, alone, may not be able to provide that coordination due to the current task overload of the staff organization.

This study hypothesizes that there is a need for an Army information task manager to oversee the lateral coordination of the information tasks into operational planning and execution. This IO specialist would be the responsible staff principal who synchronizes information activities, derived from expertise of the IO elements' capabilities, capacity, and related IO activities, and given the *reciprocal interdependence* of the information tasks. In short, the combined performance and effectiveness of the staff organization requires this form of lateral coordination to synchronize the interdependent information tasks.

B. PURPOSE, SCOPE, AND METHOD OF THIS STUDY

1. Purpose

Information is elemental to military power. It enables commanders and other leaders to effectively execute the six warfighting functions.[8] Commanders use information to: develop a common situational understanding, to enable battle command; and, to affect the operational environment.

The purpose of this thesis is to determine whether the U.S. Army is adequately prepared and organizationally structured at the operational and tactical levels of warfare and command to execute synchronous information tasks in light of recent doctrinal changes. Given the *reciprocal interdependence* of the U.S. Army's doctrinal 'information tasks,' this thesis hypothesizes that there is a need for a centralized Army information task lateral coordinator to oversee the coordination and synchronization of the information tasks into operational planning and execution.

2. Scope

The scope of this thesis is limited to information activities conducted at the U.S. Army Operational and Tactical levels of warfare and command:

---

[8] Department of the Army, *Field Manual 3-0, Operations,* 27 February 2008, (Washington, D.C.: Headquarters, Department of the Army, 2008), pp. 4-3 - 4-7, https://akocomm.us.army.mil/usapa/doctrine/DR_pubs/dr_aa/pdf/fm3_0.pdf (accessed 5/15/08). A *warfighting function* is a group of tasks and systems (people, organizations, information, and processes) united by a common purpose that commanders use to accomplish missions and training objectives.

The *Operational* level is the level of war at which campaigns and major operations are planned, conducted, and sustained to accomplish strategic objectives within theaters or operational areas. Activities at this level link tactics and strategy by establishing operational objectives needed to accomplish the strategic objectives, sequencing events to achieve the operational objectives, initiating actions, and applying resources to bring about and sustain these events. These activities imply a broader dimension of time or space than do tactics and they ensure the logistic and administrative support of tactical forces, and provide the means by which tactical successes are exploited to achieve strategic objectives.[9]

The *Tactical* level of war is the level at which battles and engagements are planned and executed to accomplish military objectives assigned to tactical units or task forces. Activities at this level focus on the ordered arrangement and maneuver of combat elements in relation to each other and to the enemy to achieve combat objectives.[10]

3. Method

In preparation for the work on this thesis, I reviewed a significant body of academic and professional research on the structure and behavior of Army organizations at the operational and tactical levels of warfare and planning. Evidence was gathered from organizational documentation,

---

[9] Department of the Army, *Field Manual 1-02, Operational Terms and Graphics,* 21 September, 2004, (Washington, D.C.: Headquarters, Department of the Army, 2004), pp. 1-138 - 1-139, https://akocomm.us.army.mil/usapa/doctrine/DR_pubs/dr_aa/pdf/fm1_02.pdf (accessed 5/21/08).

[10] Ibid., p. 1-182.

organizational archival records, and direct observation. As the organizational precepts of the 2008 FM 3-0 have not been fully saturated and implemented, some assumptions have been made as to how Army units at the tactical and operational levels of command will interpret the doctrinal guidance. Set against the Military Decision Making Process (MDMP) and analyzed through the degree of lateral processes between the doctrinal functional cells responsible for information tasks, evaluative criteria will be derived from subjective friction points inherent in nominating and synchronizing information tasks during the operations process. The 2008 FM 3-0 organizational design to affect the information dimension will be evaluated for its effectiveness to laterally coordinate numerous information tasks. A hybrid model combining the beneficial aspects of the 2008 and 2001 organizational designs will be introduced that hypothesizes that information tasks can best be synchronized and accomplished by the assistance of an information task coordinator, either the existing G/S-7 Information Operations officer, or a designated G/S-3 liaison.

C. THESIS ORGANIZATION

The thesis is organized into five chapters. Chapter I is the introduction where the thesis purpose is identified. This is preceded by a brief discussion of the mission and tasks of information operations assigned by the Department of Defense and formalized in Joint and U.S. Army publications. Additional examples are provided to illustrate symptoms of desynchronized information operations that can negatively affect military operations. Finally, the scope of

the thesis limits the research to organizations executing information tasks at the operational and tactical levels of Army warfare and command.

Chapter II provides the reader a brief literature review regarding the relationship between U.S. Army Missions, Operations, and Tasks. The integration of Army information tasks into the operations process, as well as a Joint and Army Doctrine description, and the inherent flexibility of Commanders to accomplish their mission within the parameters of doctrine will be explored.

In Chapter III, the Army information tasks are placed into the context of FM 3-0 and the execution of those tasks by the information functional coordination cells of responsibility. Descriptions of each coordination cell and each of their information capabilities are identified in this chapter.

Chapter IV provides the reader an understanding of organizational design and introduces a combined open systems model developed for this analysis. This chapter builds upon previously introduced precepts of how the U.S. Army accomplishes information tasks at the operational and tactical levels of warfare and planning. Set against the Military Decision Making Process (MDMP) and analyzed through the degree of lateral processes between the functional cells responsible for information tasks, evaluative criteria will be derived from subjective friction points inherent in nominating and synchronizing information tasks during the operations process. The 2008 FM 3-0 organizational design will be evaluated for its effectiveness to laterally coordinate information tasks. Determining how the various

components in an organization that are responsible for information tasks interact and adapt to achieve the output goal is an objective of this chapter.

Finally, Chapter V contains observations from the lateral processes analysis and provides recommendations for organizing Army operational and tactical units executing information tasks. The hypothesis contends that a hybrid of the 2008 FM 3-0 organizational design and its 2001 predecessor's design will best synchronize the accomplishment of the interdependent information tasks, producing a structural arrangement that will be most effective in incorporating information tasks into the complex operational environment.

The hybrid model will be further analyzed that contends that information tasks can best be synchronized and accomplished by the assistance of an information task coordinator, the existing G/S-7 Information Operations Officer, or by a chosen G/S-3 liaison. These recommendations are necessarily limited and are suggestive. They are based on limited resources and a moderate level of knowledge of training procedures and mission requirements. However, they should be sufficient to provoke discussion.

THIS PAGE INTENTIONALLY LEFT BLANK

II. U.S. ARMY MISSIONS, OPERATIONS, AND TASKS

This chapter provides a brief literature review regarding the relationship between U.S. Army Missions, Operations, and Tasks. The integration of Army information tasks into the operations process, as well as a Joint and Army Doctrine description, and the inherent flexibility of Commanders to accomplish their mission within the parameters of doctrine will be explored.

A. MISSION, OPERATION, AND TASK RELATIONSHIP

An Army mission establishes the requirement to perform tasks and provides the context for each task performance, to include the conditions under which a task must be performed. It determines where and when a task must be performed. Finally, it determines the degree to which a task must be performed, as stated in the concept of the operation, and provides a way to understand precisely how the performance of a task contributes to mission success.

Full spectrum operations is the term of the Army's operational concept. The components of full spectrum operations are offense, defense, stability, and civil support. The operational concept, portrayed in the figure below, is the foundation for all Army doctrine. The goal of full spectrum operations is to enable the Army to defeat an enemy on land and establish the conditions that attains the higher headquarters commander's, or joint force commander's end state.

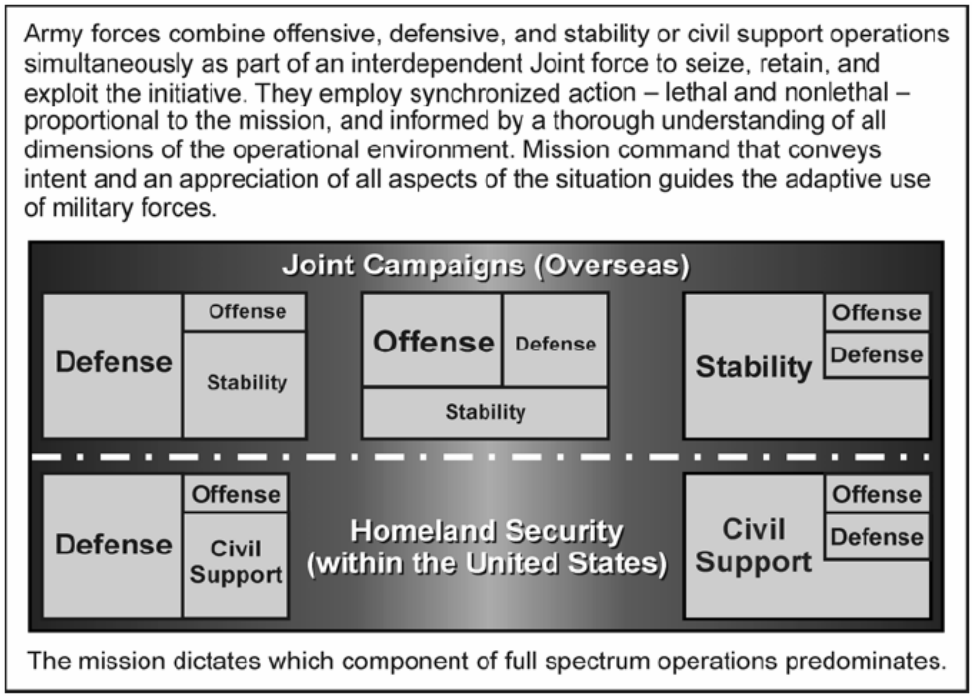

Figure 3. The Army's Operational Concept.[11]

Understanding the relationship of mission, operation, and task is important to the successful synchronization of Army informational tasks. The mission establishes the requirement to perform tasks and provides the context for each task performance, including the conditions under which a task must be performed. It determines where and when a task must be performed and further determines the degree to which a task must be performed in accordance with the concept of the operation.

The synchronization between mission, operation, and tasks is coordinated through mission analysis and subsequent steps of the Military Decision Making Process. The product of the analysis is the identification of operations and the

[11] Department of the Army, *Field Manual 3-0, Operations,* 27 February 2008, p. 3-1.

physical, informational, and cognitive tasks that must be performed in a synchronistical manner for mission success.

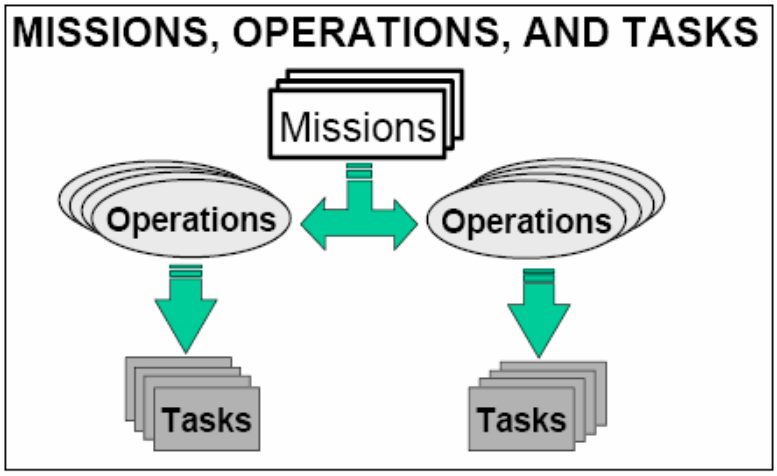

Figure 4. Relationship of Missions, Operations, and Tasks.[12]

The Army's operational concept is the core of its doctrine and that doctrine drives the mission analysis and execution of a plan, such as informational or influence operations. Doctrine is a guide to action, not hard and fast rules. Doctrine provides a common frame of reference across the military. It helps standardize operations, facilitating readiness by establishing common ways of accomplishing military tasks.

B. INTEGRATING ARMY INFORMATION TASKS INTO THE OPERATIONS PROCESS

Conducting operations that influence the enemy's will to fight is as old as warfare itself. Information Operations have been applied throughout military history, and its

[12] Joint Chiefs of Staff, *Chairman of the Joint Chiefs of Staff Manual CJCSM 3500.04C, Universal Joint Task List (UJTL),* 1 July 2002, (Washington, D.C.: Joint Staff, 2002), pp. A-7 - A-8, http://www.dtic.mil/doctrine/jel/cjcsd/cjcsm/m350004c.pdf (accessed 3/03/08).

present application continues to grow as the U.S. increases its reliance on information as a weapon and commodity. Psychological operations, operations security, military deception, physical destruction, and electronic warfare were viable tools of Army commanders during World War II. The Gulf War demonstrated the benefit of employing these elements together and synchronizing them with ground operations.

In the 1990s, a concept called Information Operations (or Information Warfare) began to take hold, first in the Joint community and then in the U.S. Army. U.S. Operations in the Balkans posed renewed challenges to the US military as it strove to change attitudes and perceptions of combatant and non-combatants as the military enforced United Nations and NATO mandates concerning Bosnia-Herzegovina and Kosovo.

The shaping operations conducted during this period of military operations included targeting key leaders on both sides to modify behaviors prior to critical events such as elections. The maneuver forces received some IO-capable assets to non-kinetically influence local leaders and the population. Some of the assets employed were tactical psychological operations teams, public affairs detachments, civil affairs teams, combat camera teams, medical treatment teams, unit commanders, and patrols. The continual use of IO in an integrated manner with maneuver operations proved successful in shaping the operational environment and defusing several potentially volatile situations. Visualizing the information domain through standard military procedures such as the Military Decision Making Process

(MDMP), Intelligence Preparation of the Battlefield (IPB), and targeting was effective in the overall success of operations.[13]

The Army codified the concept of Information Operations – the act of protecting and using information while denying the enemy the ability to do the same – in the 1996 edition of FM 100-6, *Information Operations*.[14] Subsequently in 1999, the Army created the Information Operations Career Field to provide commanders with a dedicated IO staff to ensure units plan and execute IO in a coordinated manner. Officers are typically assessed while at the rank of captain from one of many Army branches, for example Armor, Infantry, Field Artillery, and designated Functional Area 30 (FA30) Information Operations officers. Currently, there is one required training course, the twelve-week IO Officer Qualification Course at Fort Leavenworth, Kansas.[15]

In 2001, FM 3-0, *Operations*, first designated information as an element of combat power. U.S. Army Information Operations is the employment of the core capabilities of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military

---

[13] Marc J. Romanych, "Tactical Information Operations in Kosovo," *Military Review* (September-October, 2004), www.au.af.mil/au/awc/awcgate/milreview/romanych.pdf (accessed 6/17/2008).

[14] Department of the Army, *Field Manual 100-6, Information Operations,* 27 August 1996, (Washington, D.C.: Headquarters, Department of the Army, 1996), http://www.iwar.org.uk/iwar/resources/usarmyio/fm100-6.pdf (accessed 5/16/08).

[15] U.S. Army Information Operations Proponent, U.S. Army Combined Arms Center, *Fact Sheet: Functional Area 30 Qualification Course (FA30 QC),* 15 October 2008, (Fort Leavenworth, Kansas: U.S. Army Combined Arms Center, 2008).

deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to include Public Affairs (PA) and Civil Affairs (CA) to affect or defend information and information systems, and to influence decisionmaking.[16]

IO is particularly relevant in irregular warfare because it is used to influence populations, which are the center of gravity in an insurgency. Colonel Ralph O. Baker, a Brigade Combat Team Commander in Operation Iraqi Freedom with responsibilities in a volatile area of Baghdad, discussed the significant role of IO in Operation Iraqi Freedom:

> IO was going to be one of the most vital tools (along with human intelligence) I would need to be successful in a counterinsurgency (COIN) campaign. COIN operations meant competing daily to favorably influence the perceptions of the Iraqi population in our area of operations.[17]

Army IO officers are the supporting staff who plan, implement, and assess information tasks for combat units in Iraq from *Multi-National Force - Iraq* down to the battalion level. Though under-resourced and still being developed, the Army IO organization will bear greater responsibility for the success or failure of information dominance and

---

[16] Department of the Army, *Field Manual 3-13, Information Operations: Doctrine, Tactics, Techniques, and Procedures,* 28 November 2003, (Washington, D.C.: Headquarters, Department of the Army, 2003), Introduction, https://akocomm.us.army.mil/usapa/doctrine/DR_pubs/dr_aa/pdf/fm3_13.pdf (accessed 5/16/08).

[17] Ralph O. Baker, "The Decisive Weapon: A Brigade Combat Team Commander's Perspective on Information Operations." *Military Review* (May-June, 2006), p. 13, http://www.army.mil/professionalwriting/volumes/volume4/july_2006/7_06_3.html (accessed 6/17/2008).

influence in military operations by enabling commanders to use and integrate IO into all operations.

The 2008 edition of FM 3-0 reaffirms that "In modern conflict, information has become as important as lethal action in determining the outcome of operations"[18] and that commanders must integrate information "in full spectrum operations as carefully as fires, maneuver, protection and sustainment."[19]

C. INFORMATION OPERATIONS OBJECTIVE

The objective of the employment of Army IO is to gain and maintain *Information Superiority*,[20] a condition that allows commanders to seize, retain, and exploit the initiative. It facilitates more effective decisionmaking and faster execution. IO involve constant efforts to deny adversaries the ability to detect and respond to friendly operations, while simultaneously retaining and enhancing friendly force freedom of action. When expeditiously exploited, IO provides a potent advantage that facilitates rapid military success with minimal casualties. Effective IO and information management allow commanders to take advantage of opportunities, while denying adversary

---

[18] Department of the Army, *Field Manual 3-0, Operations,* 27 February 2008, p. 4-3.

[19] Ibid., p. 7-1.

[20] Joint Chiefs of Staff, *Joint Publication 1-02, DOD Dictionary of Military and Associated Terms,* 12 April 2001, as Amended through 30 May 2008, (Washington, D.C.: Joint Staff, 2001), p. 262, http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf (accessed 4/23/08). Information Superiority is the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

commanders the information needed to make timely and accurate decisions or leading them to make decisions favorable to friendly forces.

Commanders do not conduct IO simply for the sake of doing IO. Effective IO is an integrated effort that synchronizes the effects of IO elements and related activities to accomplish specific objectives designated by the commander. It is the means commanders use to mass the effects of the information element of combat power.

Focused IO, synchronized with effective information management and intelligence, surveillance, and reconnaissance, enable commanders to gain and maintain information superiority.[21] IO is a prime means for achieving information superiority, the operational advantage achieved by an uninterrupted flow of information while denying the enemy's ability to do the same.[22]

Information operations are characterized as offensive or defensive in nature. The Army defines offensive information operations as "the integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect enemy decision makers or to influence others to achieve or promote specific objectives." Army doctrine allows for commanders to use all elements of IO offensively. Defensive information operations are "the integration and coordination of policies and procedures, operations, personnel, and technology to protect

---

[21] Department of the Army, *Field Manual 3-0, Operations,* 27 February 2008, p. 7-1.

[22] Ibid., p. 7-1.

and defend friendly information and information systems."[23] In the current global, information dimension; maneuver units, with the assistance of IO trained officers, should look to incorporate offensive and defensive information operations daily into the mission. Not just as an afterthought.

D. DOCTRINAL FRAMEWORK

The term "doctrine," as a military concept, has an expansive meaning. Knowledge and understanding of doctrine are essential for effective operations on the battlefield. Doctrine provides the framework and principles to cope with the unexpected. Moreover, it provides a common language and perspective so leaders can communicate effectively with one another.

Consider the following discussion of doctrine contained in the 2008 FM 3-0:

> Ours is a doctrinally-based Army. FM 3-0 provides the intellectual underpinnings that lie at the core of how our Army will organize, train, equip, and conduct operations in this new environment…[24] Doctrine is a guide to action, not a set of fixed rules. It combines history, an understanding of the operational environment, and assumptions about future conditions to help leaders think about how best to accomplish missions.[25]

---

[23] Department of the Army, *Field Manual 3-13, Information Operations: Doctrine, Tactics, Techniques, and Procedures,* 28 November 2003, pp. 1-14 - 1-18.

[24] Department of the Army, *Field Manual 3-0, Operations,* 27 February 2008, Foreword.

[25] Ibid., p. D-1.

Military doctrine is the concise expression of how military forces contribute to campaigns, major operations, battles, and engagements. Doctrine provides a common frame of reference for independent and interdependent tasks across the military. It helps standardize operations, facilitating readiness by establishing common ways of accomplishing military tasks, such as informational and influence tasks.

Doctrine influences all aspects of the U.S. military. It provides a common language and a common understanding of how the U.S. Armed Forces conduct operations. Doctrine, like history, requires significant analysis and elucidation before it is written and accepted, which takes time. Doctrine is evolutionary. However, when it is written and published it should represent the military's best guess of how our leaders and soldiers should approach warfighting. This description of the function of doctrine in the U.S. military builds upon similarly accepted conceptions of doctrine still held by commentators today:

> Doctrine is an approved, shared idea about the conduct of warfare that undergirds an army's planning, organization, training, leadership style, tactics, weapons, and equipment. These activities in preparation for future war lie at the heart of the military profession in modern societies. When well-conceived and clearly articulated, doctrine can instill confidence throughout an army. An army's doctrine, therefore, can have the most profound effect on its performance in war.[26]

---

[26] Paul H. Herbert and U.S. Army Command and General Staff College, Combat Studies Institute, *Deciding What Has to be Done: General William E. DePuy and the 1976 Edition of FM 100-5, Operations*, Vol. 16 (Fort Leavenworth, Kan.: Combat Studies Institute, U.S. Army Command and General Staff College, 1988), p. 3, http://www-cgsc.army.mil/carl/resources/csi/Herbert/Herbert.asp#3 (accessed 16/8/08).

Joint Forces doctrine provides a common language and a common understanding of how the Armed Forces conduct operations, and it is applicable to the joint staff, commanders of combatant commands, sub-unified commands, joint task forces, subordinate components of these commands, and the Services, to include the U.S. Army. Army doctrine continues the continuity by providing a common understanding of how Army forces conduct operations.

E. U.S. ARMY DOCTRINE

Army doctrine is designed to be detailed enough to guide operations, yet flexible enough to allow commanders to exercise initiative when dealing with specific tactical and operational situations. Recent transformations of U.S. Army organizations necessitated transforming the doctrine that supports their tactical and operational-level tasks and functions.

The Army has two Capstone Field Manuals — FM 1, *The Army*, and FM 3-0, *Operations* — that form the apex of the Army's doctrine hierarchy. Together, they establish the framework for a range of supporting doctrine. Army keystone doctrine is organized around foundations established in FM 3-0. Supporting manuals provide additional detail for keystone manuals.

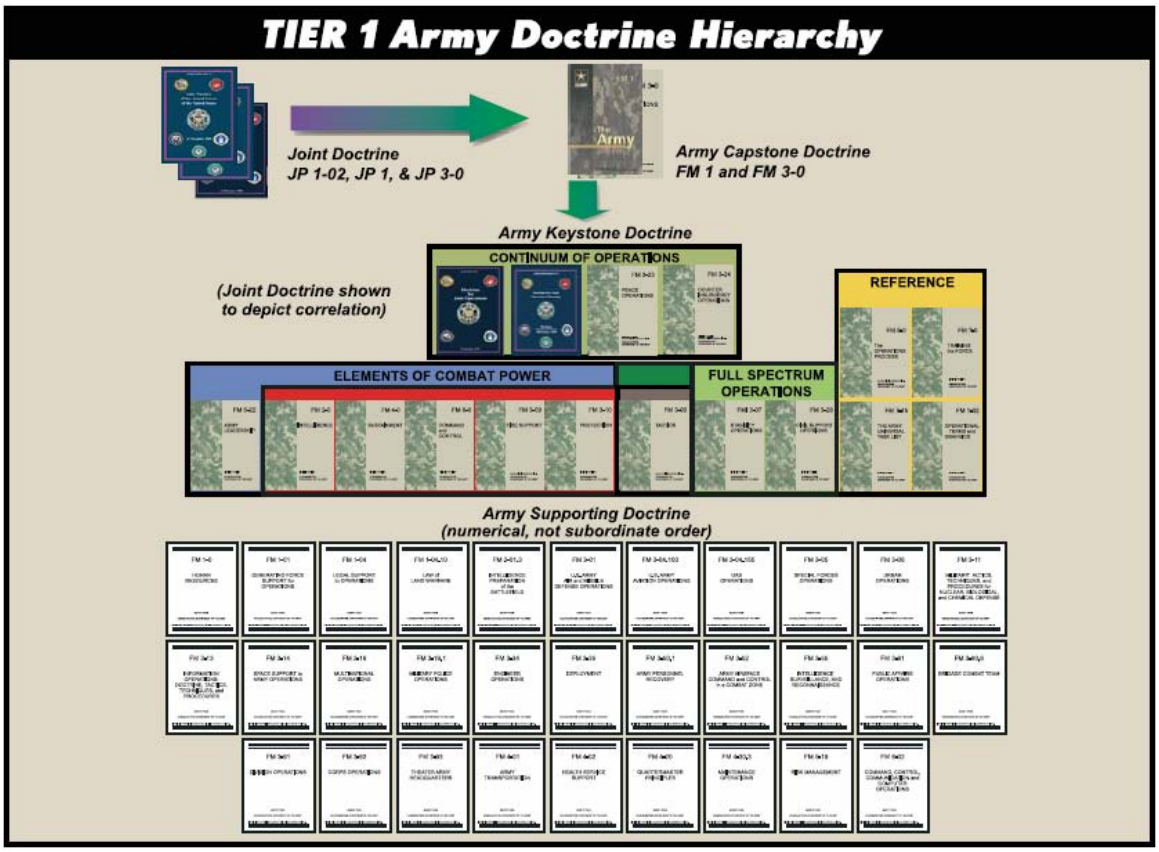

Figure 5. The Tier 1 Army Doctrine Hierarchy.[27]

The Army's Field Manual numbering system, which mirrors the Joint system, aligns Army doctrine with Joint doctrine. The Army's warfighting doctrine is structured into a two-tiered hierarchy to provide for development and implementation of Army doctrinal publications. Tier 1 is the highest-level, with the majority of the field manuals directly linked to Joint doctrine as indicated by a parallel numbering system. In addition to the capstone publications FM 1 and FM 3-0, approximately 48 other Tier 1 FMs and

[27] Department of the Army, Office of the Deputy Chief of Staff, G8, *2007 Army Modernization Plan* (Washington D.C.: Office of the Deputy Chief of Staff, G8, 2007), p. 20, http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=ADA468000&Location=U2&doc=GetTRDoc.pdf (accessed 8/20/08).

supporting publications offer broad perspectives on Army operations in Joint campaigns. Tier 2 Doctrine, comprised of 550 FMs, capture the bulk of proponent, lower-level organizational FMs, most of which are narrower in scope than Tier 1 FMs.

As a Capstone Field Manual, FM 3-0 establishes the Army's fundamental principles for applying land power as part of an interdependent joint force. It provides a framework for action and decision making at all levels. The aim is to establish guidelines for leaders to direct operations while allowing enough freedom for bold, creative initiative in any situation. As Tier 1 doctrine, FM 3-13, *Information Operations*, is the Army's overarching IO publication that was built on the foundation set in the 2001 FM 3-0's Chapter 11, "Information Superiority," but is now subordinate to the new ideas of Information Superiority as set my the 2008 FM 3-0.

F. CONCLUSION

The Army's adherence the present doctrine, to include the 2008 FM 3-0 is non-negotiable. Yet, Army doctrine is designed to be detailed enough to guide operations, yet flexible enough to allow commanders to organize their staffs as they see most advantageous to gain the initiative when dealing with specific tactical and operational situations. Commanders' retain the authority to organize their staffs and their functions within the parameters of Army doctrine.

THIS PAGE INTENTIONALLY LEFT BLANK

III. U.S. ARMY INFORMATION TASKS

Building on the literature review, Joint and Army Doctrine description, and the integration of Army information tasks into the operations process, this chapter explains how the Army information tasks are placed into the context of the 2008 FM 3-0 and the execution of those tasks by the functional coordination cells of responsibility. Descriptions of each coordination cell and each of their information capabilities are identified in this chapter.

A. FUNCTIONAL COORDINATION CELLS

As the collection of the *Core*, *Supporting* and *Related* information capabilities, the term 'Information Operations' has fallen out of favor in the U.S. Army. The contention stems from the fact that information operations and its constituents are considered an aggregated whole of the capabilities that were previously well-established and were previously treated as largely independent.

Meanwhile, Joint Doctrine still defines information operations as the *Core*, *Supporting* and *Related* capabilities of information operations.[28] The five core capabilities are Psychological Operations (PSYOP), Military Deception (MILDEC), Operational Security (OPSEC), Electronic Warfare (EW), and Computer Network Operations (CNO). The first three core capabilities have long existed as part of military operations and the latter two have recently been integrated into contemporary military operations. The capabilities

[28] Joint Chiefs of Staff, *Joint Publication 3-13, Information Operations,* February 13 2006.

supporting information operations include information assurance (IA), physical security, physical attack, counterintelligence (CI), and combat camera (COMCAM), and are seen as directly or indirectly involved in shaping the information dimension of the operational environment. The related capabilities constitute public affairs (PA), civil-military operations (CMO), and defense support for public diplomacy (DSPD). The core capabilities are applicable at all levels of warfare, tactical, operational and strategic, whereas the supporting capabilities dominate the operational and the tactical levels and the related capabilities dominate the strategic and the operational levels.

Army doctrine uses the joint definition of “information operations” as well as all of the capabilities that compose IO; however, Army doctrine categorizes IO capabilities differently from joint doctrine. Army doctrine describes affecting the Information Dimension of the Operational Environment in terms of five IO tasks:

- Information Engagement
- Command and Control Warfare
- Information Protection
- Operations Security
- Military Deception

Responsibilities for information operations tasks are as follows:

- Information Engagement – Information Engagement Cell
- Command and Control Warfare – Fires Cell
- Information Protection – C4OPS Cell
- Operations Security – Protection Cell
- Military Deception – Plans Cell

While this chapter briefly discusses the execution of the five IO tasks by the individual proponents and

capabilities in each of the respective functional coordination cells as codified in the 2008 FM 3-0, a comprehensive description of each of the functional coordination cell members and capabilities, previously defined as IO *core*, *supporting* and *related* capabilities, can be found in the Appendix.

Army IO Tasks	IO Capabilities	Staff Responsibility	Functional Coordinating Cell	Intended Effects	Integrating Process
Military Deception	Military Deception	G-5	Plans	Exploit, Deceive	Operations Process
Information Engagement	PSYOP Combat Camera Defense Support to Public Diplomacy	PSYOPS G-7	Information Engagement	Influence and Inform	
	Public Affairs	PAO		Inform	
Command and Control Warfare	Electronic Attack Computer Network Attack Electronic Warfare Support Computer Network Exploitation	G-2 G-3	Fire Support	Search, Intercept, Identify, Locate, Deceive, Disrupt, Deny, Degrade, Destroy	
	Physical Attack	G-3		Deceive, Disrupt, Deny, Degrade, Destroy	
Information Protection	Information Assurance Computer Network Defense Electronic Protect	G-6	C4OPS	Detect, Protect, Defend	
Operations Security	Operations Security Physical Security	G-3	Protection	Secure, Deny	
	Counterintelligence	G-2		Protect	

Figure 6. Army Information Tasks.[29]

B. INFORMATION ENGAGEMENT FUNCTIONAL COORDINATION CELL

Information engagement is the 'Integrated employment of public affairs to inform U.S. and friendly audiences;

[29] Combined Arms Doctrine Directorate (CADD), *Army Doctrine Update,* 24 February 2007 (Fort Leavenworth, Kansas: US Army Combined Arms Center, 2007), http://asc.army.mil/docs/transformation/Army_Doctrine_Update_FM501_FM30.pdf (accessed 8/20/08).

psychological operations, combat camera, U.S. Government strategic communication and defense support to public diplomacy, and other means necessary to influence foreign audiences; and, leader and Soldier engagements to support both efforts.'[30] The Information Engagement Functional Coordination Cell is charged with synchronizing a consistent information engagement strategy that communicates information, builds trust and confidence, influences perceptions and behavior, and promotes support for Army, coalition and partnered host nation security forces. The staff proponents and capabilities of the Information Engagement Cell include: Leader and Soldier Engagement, Public Affairs (PA), Psychological Operations (PSYOP), Combat Camera (COMCAM), and 'Strategic Communication and Defense Support to Public Diplomacy.' The primary staff responsibility for the conduct of the Information Engagement functional cell is the G/S-7 Information Operations Officer with Public Affairs, PSYOP and G/S-9 Civil Affairs support within the information engagement cell.

C. COMMAND AND CONTROL WARFARE FUNCTIONAL COORDINATION CELL

Command and control warfare is 'The integrated use of physical attack, electronic warfare, and computer network operations, supported by intelligence, to degrade, destroy, and exploit the adversary's command and control system or to deny information to it.'[31] The staff proponents and capabilities of the Command and Control Warfare Cell

[30] Department of the Army, *Field Manual 3-0, Operations,* 27 February 2008, pp. 7-3 - 7-5.

[31] Ibid., p. 7-6.

include: ‘Physical Attack,’ Electronic Attack (EA), Electronic warfare Support (ES), Computer Network Attack (CNA), and Computer Network Exploitation (CNE). The primary staff responsibility for the conduct of the Command and Control Warfare functional cell is the G/S-3 Operations Officer with G/S-2 Intelligence Officer support within the fires cell.

D. INFORMATION PROTECTION FUNCTIONAL COORDINATION CELL

Information Protection is the ‘Active or passive measures that protect and defend friendly information and information systems to ensure timely, accurate, and relevant friendly information. It denies enemies, adversaries, and others the opportunity to exploit friendly information and information systems for their own purposes.’[32] The staff proponents and capabilities of the Information Protection Cell include: Information Assurance (IA), Computer Network Defense (CND), and Electronic Protection (EP). The primary staff responsibility for the conduct of the Information Protection functional cell is the G/S-6 Communications Officer within the Network Operations Cell.

E. OPERATIONS SECURITY FUNCTIONAL COORDINATION CELL

Operations security identifies essential elements of friendly information and evaluates the risk of compromise if an adversary or enemy obtains that information. This analysis compares the capabilities of hostile intelligence systems with the activities and communications of friendly

[32] Department of the Army, *Field Manual 3-0, Operations,* 27 February 2008, p. 7-7.

forces and friendly information vulnerabilities. The analysis focuses on critical information that an adversary could interpret or piece together in time to be useful. Once identified, operations security experts prioritize friendly vulnerabilities and recommend countermeasures and other means of reducing the vulnerability.[33] The staff proponents and capabilities of the Operations Security Cell include: Operations Security (OPSEC), Physical Security, and Counterintelligence (CI). The primary staff responsibility for the conduct of the Operations Security functional cell is the G/S-3 Operations Officer with G/S-2 Intelligence Officer support within the protection cell.

F. MILITARY DECEPTION FUNCTIONAL COORDINATION CELL

At its most successful, military deception provokes an enemy commander to commit a serious mistake that friendly forces can exploit, there or elsewhere. However, effective military deception also introduces uncertainty into the enemy's estimate of the situation, and that doubt can lead to hesitation. Deception is a good means of dislocating an enemy force in time and space. Military deception can contribute significantly to information superiority; however, it requires integration into the overall operation beginning with receipt of mission.[34]

MILDEC in the information domain is quite different from the traditional or conventional MILDEC that involved the fusing of deception with physical tangibles on the ground; in the information age, MILDEC may achieve success

---

[33] Department of the Army, *Field Manual 3-0, Operations,* 27 February 2008, p. 7-7.

[34] Ibid., p. 7-7.

by shaping the information without too much reliance on commensurate actions in the physical domain. This ability to move away from traditional employment of MILDEC could allow it to be better integrated in information operation campaigns against terrorist organizations and networks. The importance of understanding the adversary's 'collection systems and sensors,' to absorb deception, and to correctly assess their attitudes and reactions, is an essential ingredient for a successful MILDEC operation.

The staff proponents and capabilities of the Military Deception Cell could include a cross-section of the entire staff, as MILDEC operations are planned and subjected to the same operations process as legitimate operations. The primary staff responsibility for the conduct of the Military Deception functional cell is the G/S-5 Plans Officer within the plans cell.

G. CONCLUSION

The responsibility for executing the five Army information tasks now rests within each of the staff functional cells. When properly integrated, IO can facilitate and enhance military operations across the operational spectrum. Properly employed and laterally coordinated, information operations can conserve limited resources, reduce operational risk, and significantly enhance Army mission accomplishment. Improperly coordinated, unintended consequences can create an organizational climate "where risk aversion dominates decisionmaking related to information tasks."[35]

[35] Department of the Army, *Field Manual 3-0, Operations,* 27 February 2008, p. 7-3.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. ARMY INFORMATION TASKS INTEGRATION

This chapter builds upon previously introduced precepts of how the U.S. Army accomplishes information tasks at the Operational and Tactical levels of warfare and planning. Set against the Military Decision Making Process (MDMP) and analyzed through the degree of lateral processes between the functional cells responsible for information tasks, evaluative criteria will be derived from subjective friction points inherent in nominating and synchronizing information tasks during the operations process. The 2008 FM 3-0 organizational design will be evaluated for its effectiveness to laterally coordinate these information tasks.

A. THE MILITARY DECISION MAKING PROCESS (MDMP)

The new 2008 FM 3-0 has dictated that the former concept of *information operations* now be divided into five Army *information tasks*, in regard to the work required to operate within the information dimension of the operational environment. The responsibility for executing these information tasks has been distributed to independent staff functional cells, to be ultimately synchronized through the *operations process*.[36]

The 'operations process' refers to the Military Decision Making Process (MDMP). MDMP is the current doctrinal framework to decision making and planning at the operational and tactical levels and it represents an

[36] Department of the Army, *Field Manual 3-0, Operations,* 27 February 2008, pp. 7-2 - 7-3.

analytical approach to problem solving through the concerted efforts of the commander and his staff. The decision maker is the central MDMP element, yet it is a multidimensional undertaking involving the decision maker, the operational environment, organization, planning, learning and procedures.[37]

As defined in the current FM 5-0, *Army Planning and Orders Production*, the military decision making process "is a planning model that establishes procedures for analyzing a mission, developing, analyzing, and comparing courses of action against criteria of success and each other, selecting the optimum course of action, and producing a plan or order."[38] In short, the MDMP is a seven-step analytical process. Beginning with Step 1, Receipt of Mission, and continuing through Step 7, Orders Production, the MDMP is the established doctrinal framework for problem solving used by staff organizations at the operational and tactical levels of warfare. As shown in the chart below, the MDMP considers input and analysis from across the staff to inform the commander of what he needs to make a decision as to how best to solve a problem.[39]

---

[37] Christopher R. Paparone, "US Army Decisionmaking: Past, Present and Future," *Military Review* (July-August, 2001), p. 48.

[38] Department of the Army, *Field Manual 5-0, Army Planning and Orders Production,* 20 January 2005, (Washington, D.C.: Headquarters, Department of the Army, 2005), p. 3-1, https://akocomm.us.army.mil/usapa/doctrine/DR_pubs/dr_aa/pdf/fm5_0.pdf (accessed 5/16/08).

[39] Ibid., p. 3-3.

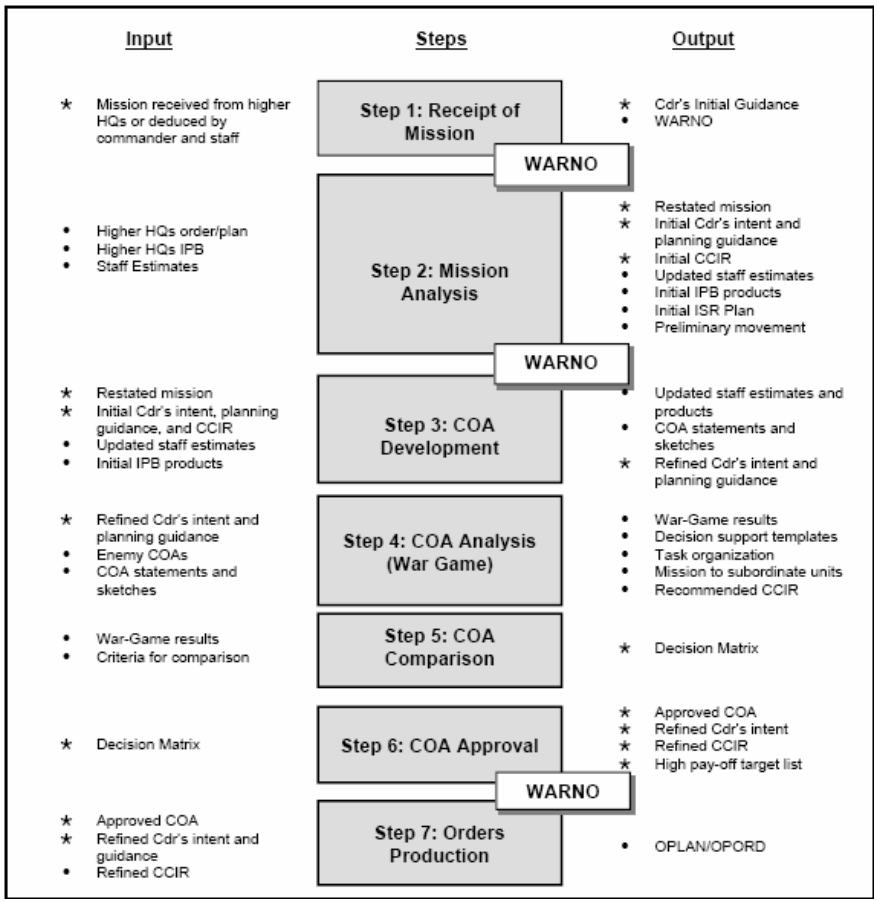

Figure 7. The Military Decision Making Process.[40]

The MDMP supports a commander's need to visualize, describe, and direct actions against a hostile, thinking enemy. Furthermore, this planning and decision making process requires synchronization and synergy of effects as current operational environments demand rapid, decisive operations with a multitude of assets that make up an Army unit's combat power. Flexibility is also instrumental in the MDMP to account for Army operations across the spectrum of conflict.

[40] Department of the Army, *Field Manual 5-0, Army Planning and Orders Production,* 20 January 2005, p. 3-3.

B. TASK PROCESSES

All organizations exist to produce something.[41] Army information tasks functional coordination cells were formed by FM 3-0 in a functional structure to seamlessly produce desired physical, informational, and cognitive effects. A *functional* structure is organized around major activity groups, such as each of the individual information tasks. Staff officers are managed together in each task to promote sharing of knowledge and specialization within the accomplishment of each task. In theory, this structure should promote standardization and reduce duplication.[42] However, this structure could become a barrier as the processes required to synchronize and de-conflict their activities across the coordination cells become necessary due to MDMP and the flexible requirements of conducting full-spectrum operations.

In his book, *Designing Organizations*, Jay R. Galbraith found that in order for an organization to accomplish short- and long-term goals, the interdependence of functional units requires coordination across departments. Thus, if functional units are interdependent, they must coordinate to function. Therefore, when an endeavor like a comprehensive approach to the information dimension of the operating environment becomes multidimensional, it may not be wise to

---

[41] The word *organization* for the purpose of this research can be a division or brigade staff. Yet, organizations are nested inside one another. Each of the functional coordination cells responsible for an Army information task represent an organization, greatly influenced by the surrounding staff organization.

[42] Amy Kates and Jay R. Galbraith, *Designing Your Organization : Using the Star Model to Solve 5 Critical Design Challenges*, 1st ed. (San Francisco: Jossey-Bass, 2007), pp. 10-11.

decentralize operations into small autonomous cells because they risk becoming uncoordinated and perform at a less than optimal or "dysfunctional" level.[43] This does not automatically mean that more complex networks are needed, because other dimensions of organizational theory must be considered before accepting that conclusion.

Recognition of Thompson's interdependence becomes paramount. Each of the five Army information tasks possesses an inherent *reciprocal interdependence* to the other tasks as they cumulatively shape the information dimension of the operational environment.[44] Specifically, in the execution of an information campaign, the output of one staff functional cell responsible for one information task could become the input to another cell accountable for another information task. In this view, the Army Information Functional Coordination Cells represent interdependent functional units, as Galbraith termed "coordinated interdependent units."[45] The recent organizational restructuring as mandated in the 2008 FM 3-0 is intended to increase the staff proponents' understanding of information's indispensable role in any operation across the full spectrum of conflict. The new design further increases the number of staff officers that will be required to develop information tasks and integrate it into full spectrum operations as

---

[43] Jay R. Galbraith, *Designing Organizations : An Executive Guide to Strategy, Structure and Process*, New and rev. ed. (San Francisco: Jossey-Bass, 2002), p. 5.

[44] Thompson, *Organizations in Action: Social Science Bases of Administrative Theory*, pp. 45-55, 52-53, 55-56.

[45] Galbraith, *Designing Organizations : An Executive Guide to Strategy, Structure and Process*, p. 5.

synergistically as it had the other elements of combat power, such as fires, maneuver, protection and sustainment.

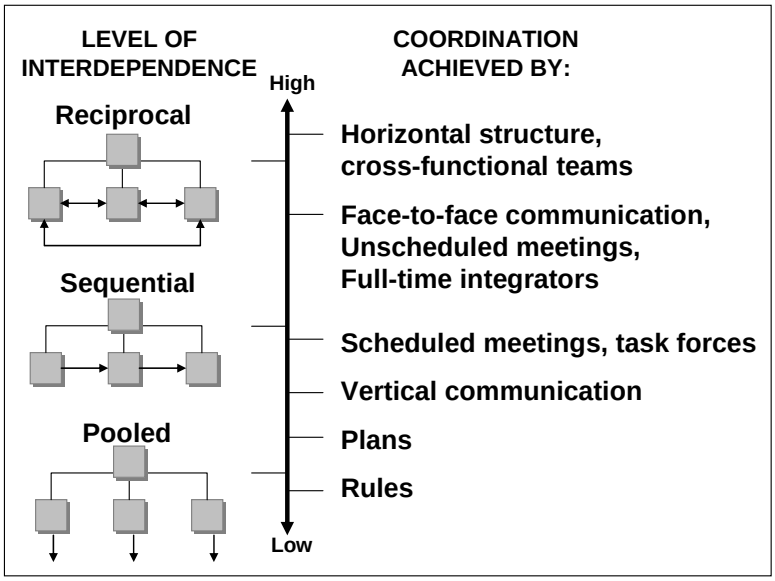

Figure 8. Primary means to achieve coordination for levels of Task Interdependence.[46]

In Army vernacular, *coordination* is "the action necessary to ensure adequately integrated relationships between separate organizations located in the same area."[47] Coordination is said to take place continuously through operations and is essential to synchronize relevant factors and effectively employ all available assets. Coordination within an Army staff ensures that staffs refine plans and

[46] Adapted from Richard L. Daft and Raymond A. Noe, *Organizational Behavior* (Mason, OH: South-Western, 2001), p. 91.

[47] Department of the Army, *Field Manual 6-0, Mission Command: Command and Control of Army Forces,* 11 August 2003, (Washington, D.C.: Headquarters, Department of the Army, 2003), p. 6-15, https://akocomm.us.army.mil/usapa/doctrine/DR_pubs/dr_aa/pdf/fm6.pdf (accessed 8/14/08).

supports MDMP by resolving problems, conflicts, and resource allocations. A fluid exchange of information is critical to successful coordination.[48]

C. LATERAL TASK CONTROL

Certainly, the autonomous construct of the information task cells could create boundaries that make it difficult for one cell to interact and synchronize information tasks with another. The organizational challenge then becomes "how to bridge these internal boundaries and integrate activities."[49] The term *process* involves the flow of information and decision procedures across the organization's structure. Processes can be either vertical through planning and staff hierarchy, or horizontal through lateral relationships. Processes that cross organizational boundaries force organizational units to work together, as Scott A. Snook asserts, "Whatever you divide, you have to put back together again; the more divided, the more effort required to rejoin. How social systems do this is what organizing is all about."[50]

In addition to processes, Amy Kates and Jay R. Galbraith identify *lateral connections* that can be used to bridge barriers erected by an organization's structure.[51] As

---

[48] Department of the Army, *Field Manual 6-0, Mission Command: Command and Control of Army Forces,* 11 August 2003, p. 6-15.

[49] Kates and Galbraith, *Designing Your Organization : Using the Star Model to Solve 5 Critical Design Challenges*, p. 17.

[50] Scott A. Snook, *Friendly Fire : The Accidental Shootdown of U.S. Black Hawks Over Northern Iraq* (Princeton, N.J.: Princeton University Press, 2000), p. 143.

[51] Kates and Galbraith, *Designing Your Organization : Using the Star Model to Solve 5 Critical Design Challenges*, pp. 17-21.

FM 3-0 dictates that the autonomous functional cells will be the functional design, the question then becomes how can the interdependent information tasks be coordinated and synchronized across departments? Developing more lateral connections across departments is often more efficient than relying on the "up-across-down" inter-departmental flow of information in hierarchical communications. These lateral connections augment the informal relations across departmental boundaries that naturally develop, to create a more formal part of the structure.

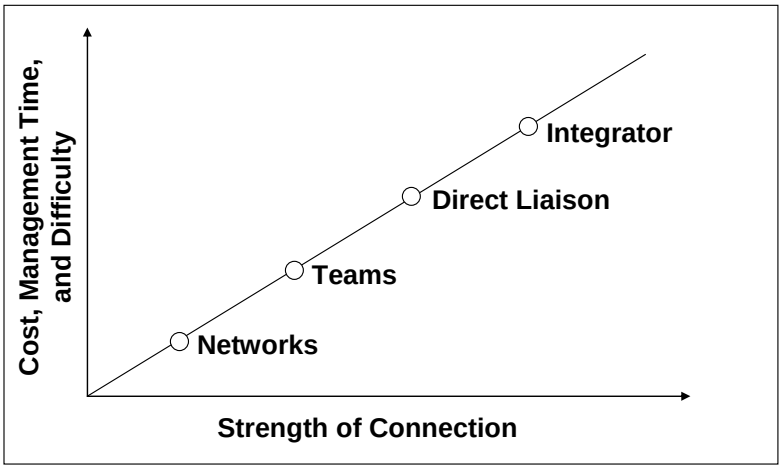

Figure 9. Lateral integrating mechanisms.[52]

One tradeoff of formal lateral connections is the transfer of some control from hierarchical schemes to more lateral, inter-departmental schemes. Some mechanisms of lateral connections employed to increase levels of lateral control are: Networks, Teams, Direct Liaison, and a full-time Integrator.

---

[52] Adapted from Kates and Galbraith, *Designing Your Organization : Using the Star Model to Solve 5 Critical Design Challenges*, p. 18; and, Jay R. Galbraith, Diane Downey and Amy Kates, *Designing Dynamic Organizations* (New York: Amacom, 2002), p. 175.

1. Networks

Networks pertain to the web of interpersonal relationships that staff officers will form across the information cells and should serve to coordinate work of information tasks informally. Kates and Galbraith assert that “healthy networks are the foundation for all other lateral connections,” thus, this initial lateral connection is inclusive in the increasingly greater levels of lateral control that follow.[53] To facilitate the required lateral coordination, Army units could create communities of practice, conduct meetings, and use technology to make knowledge sharing between the complimentary and interdependent departments possible. The planning process will certainly require numerous meetings to bring people together to collaborate information tasks and objectives. Given a constrained planning timeline and the flexible nature of full-spectrum operations, merely networking the functional coordination cells by the various planned MDMP meetings may not be sufficient enough to fully synchronize the nomination, synchronization, and execution of information tasks.

2. Teams

Teams are a group made up of part-time or full-time people from several departments set up to address a specific task. In formal project teams, there is usually a project leader assigned to coordinate group activities and department officers would delegate some authority to the

[53] Kates and Galbraith, *Designing Your Organization : Using the Star Model to Solve 5 Critical Design Challenges*, p. 17.

project leader and share collective responsibility for outcomes.[54] Teams are typically staffed by people who remain in their specialty role and devote part of their time to the team's mission.

The 2008 FM 3-0 Army information functional coordination cells are an example of full-time membership, yet part-time team execution of information tasks, as the cells' assigned staff members are responsible for more than just the information dimension of the operational environment. Teamwork and collaboration are dependent on strong mechanisms for sharing information. It is assumed that the information task teams will be flexible enough to quickly adjust to changing operational circumstances. The individual team members will be dependent on each other to nominate and finish a common information task and this requires synchronization of individual actions, and cooperation between individual team members. While focusing on the collaboration within the team, little time may be allotted to synchronize the work with adjacent information teams, potentially requiring the next higher degree of lateral connections, the *liaison*.

3. Direct Liaison

Galbraith developed various types of liaison devices on the basis of the degree of lateral inclusion in decision-making. Lateral inclusion is defined in terms of the explicitness of the horizontal decision role and authority

[54] Kates and Galbraith, *Designing Your Organization: Using the Star Model to Solve 5 Critical Design Challenges*, p. 18.

in decision making.[55] Staffs coordinate plans, execution, and adjustment decisions internally to keep operations synchronized.[56] An Army liaison role could bridge departments and have responsibility for troubleshooting, integrating, and conflict resolution. In addition to passing information, the liaison can add meaning and context to information they send and receive.[57] The G/S-3 could assign a liaison officer to bridge the information functional cells in order to synchronize information tasks, or the G/S-7 could serve this function while simultaneously serving as a member of the *Information Engagement* functional cell.

4. Integrator

An integrator provides a higher level of coordination than teams and direct liaison. An integrative role can consist of a full-time manager charged with synchronizing work across departments. The integrator can have accountability for results but does not directly manage the resources required to achieve those results. The integrator achieves power through a direct, reporting relationship to the commander. The 2001 FM 3-0 and 2003 FM 3-13 supported the legacy paradigm in which G/S-7s were responsible for coordinating all IO capabilities. In this respect, G/S-7s were referred to as integrators of IO capabilities and the accountable staff principal who synchronized information activities derived from his training, knowledge, and expertise of the full range of IO capabilities and related

---

[55] Galbraith, *Designing Complex Organizations*, p. 150.

[56] Department of the Army, *Field Manual 6-0, Mission Command: Command and Control of Army Forces,* 11 August 2003, p. 6-26.

[57] Ibid., p. 3-23.

activities. The G/S-3 could assign an operations officer to serve as the full-time information task integrator or the G/S-7 could perform the integrator role while concurrently serving as a member of the *Information Engagement* functional cell.

Although Galbraith's findings on organizational functionality derived from his examination of private sector companies, such as Hewlett-Packard and Boeing, and not Army staffs at the operational and tactical levels of war, this makes little difference from a command and control perspective. Executed independently, the interdependent nature of the tasks of the Army information functional cells requires some form of lateral coordination across those cells.

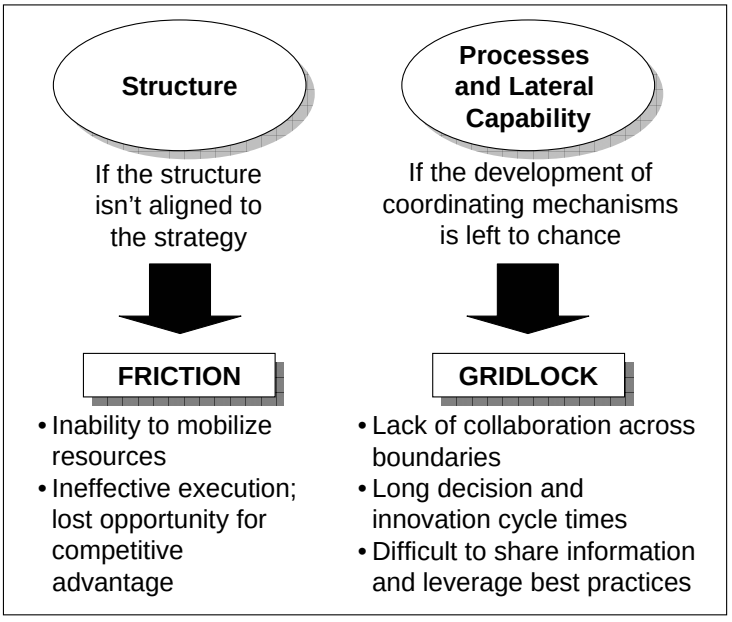

Figure 10. Unaligned organizational structure and processes.[58]

[58] Adapted from Galbraith, Downey and Kates, *Designing Dynamic Organizations*, p. 5.

In absence of this *process* of unimpeded and fluid flow of information and decision procedures across the organization's structure, the staff could likely become uncoordinated and perform at a less-than-optimal level, leading to gridlock and friction. Conversely, a framework of facilitation and coordination can promote innovation and stimulate creativity.[59]

D. INFORMATION TASK FRICTION POINTS

Placement of operational and tactical Army organizations into the context of the combined open systems model is extensive because of the complex and dynamic internal and external and variables that affect information task planning and management at those levels of warfare. In order to analyze the work to be accomplished by the staff, and the accomplishment of information tasks by the individual functional coordination cells, the Galbraith theory of *degree of lateral processes* now serves as a structure to identify six Information Tasks Friction Points. These friction points will then serve as evaluative criteria between the staff organizational structures as delineated in the 2008 FM 3-0. This organizational design, as well as a hybrid model, will be evaluated for their effectiveness to accomplish information tasks.

Full spectrum operations demand a flexible approach to planning.[60] During the MDMP, critical informational dimension requirements present themselves that require

---

[59] Kates and Galbraith, *Designing Your Organization : Using the Star Model to Solve 5 Critical Design Challenges*, p. 169.

[60] Department of the Army, *Field Manual 5-0, Army Planning and Orders Production,* 20 January 2005, p. 1-2.

identifying, analyzing, and understanding of those publics and actors whose perceptions, attitudes, beliefs, and behaviors will affect the unit's mission.

Information Tasks Friction Points	Steps of the Military Decision Making Process
1. Commander's conceptualization of the Information Dimension of the Operational Environment at start of the operations process (MDMP)	Step 1: Receipt of Mission
2. Analysis of information tasks inherent in shaping and decisive operations to meet Commander's Intent	Step 2: Mission Analysis
3. Synchronization of information tasks throughout operations process	Step 3: COA Development
	Step 4: COA Analysis (War Game)
	Step 5: COA Comparison
	Step 6: COA Approval
4. Staff roles, training, and bounded rationality	Step 7: Orders Production
5. Flexibility during current operations 6. Coordination with Higher Headquarters and Joint community	(Military Operations)

Table 1. Information Tasks Friction Points during the MDMP.[61]

The input of Step 1. of the MDMP, *Receipt of Mission*, is receipt of the higher headquarters or Joint headquarters Operations Plan (OPLAN), Operations Order (OPORD), or Warning Order (WARNO). This step leads us to the first information task friction point:

1. Commander's Orientation to Information Dimension

The commander's conceptualization of the information dimension at the start of the operations process is critical to his understanding of the operational environment. Because

[61] Information Tasks Friction Points encountered during the MDMP.

military operations are fundamentally dynamic, this visualization not only forms the basis of commanders' initial situational understanding, it continually must be validated throughout the operations process.[62]

Upon receipt of the mission, the commander and staff perform an initial assessment. Based on this assessment, the commander issues the initial guidance to begin the planning process.[63] Commanders describe their visualization in the form of their intent. During planning, the commander's intent drives the MDMP. The staff uses it to develop courses of action that conform to how the commander wants to achieve the end state.[64]

The commander is required to consider all operational aspects of the environment, to include the information dimension, in a singular plan from its inception. The commander and organizational staff must conceptualize those cognitive effects likely to produce the desired end state, and then design an operation with physical actions, words, and images synchronized in such a way as to best promote the desired outcomes. In other words, commanders must "match information tasks with actions on the ground in their concept of operation."[65]

---

[62] Department of the Army, *Field Manual 3-0, Operations,* 27 February 2008, p. 5-4.

[63] Department of the Army, *Field Manual 5-0, Army Planning and Orders Production,* 20 January 2005, pp. 3-12 - 3-15.

[64] Department of the Army, *Field Manual 6-0, Mission Command: Command and Control of Army Forces,* 11 August 2003, p. 4-8.

[65] Department of the Army, *Field Manual 3-0, Operations,* 27 February 2008, p. 7-2.

The staff is instrumental in enabling the commander's clear understanding of friendly force's current state in relation to the adversary and the environment. Accurate situational understanding of the information dimension is critical to focus the information element of combat power to accomplish the mission.

2. Analysis of Necessary Information Tasks

The commander builds on his visualiztion by analyzing the information tasks inherent in shaping and decisive operations to meet his intent. Step 2 of the MDMP, Mission Analysis, consists of 17 tasks to "help commanders refine their situational understanding and determine their mission."[66] One of the most critical tasks of Mission Analysis is the Intelligence Preparation of the Battlefield (IPB) in which intelligence requirements are generated that are essential to staff estimates, targeting, and the rest of the decision making process. A significant step of the IPB is to describe the battlefield's effects. This step involves evaluating all aspects of the environment, to include an analysis of information tasks inherent in shaping and decisive operations planning to meet the commander's intent. Identifying all of the opportunities the operating environment presents, such as the ability of actors in the information dimension to effect friendly decision making and operations, is critical at this point in the MDMP in order to generate implied information tasks that were not explicitly stated in the higher headquarters' order. Early

[66] Department of the Army, *Field Manual 5-0, Army Planning and Orders Production,* 20 January 2005, p. 3-15.

dissemination of IO-related information tasks and requirements facilitates synchronization and collaborative planning.

3. Synchronization of Information Tasks

The synchronization of information tasks throughout operations process is critical in mobilizing resources, collaboration, and the synergistic application of information capabilities to achieve the desired effects. In developing courses of action, staff members determine the doctrinal requirements for each type of mission.[67] Some information tasks, such as those that use fire support, intelligence, or maneuver assets, require tradeoffs with other maneuver options.[68] The staff considers these trade-offs through a collaborative process to generate options during course of action analysis.

When developing information tasks, the staff considers all IO elements and determines, based on available assets and resources, what contributions each can achieve to decisively achieve an operational objective. Tasks of several IO elements and related activities may contribute to accomplishing a single operational objective, or a single information task may support more than one operational objective.[69] This interdependence of the information

---

[67] Department of the Army, *Field Manual 5-0, Army Planning and Orders Production,* 20 January 2005, p. 3-33.

[68] Department of the Army, *Field Manual 3-13, Information Operations: Doctrine, Tactics, Techniques, and Procedures,* 28 November 2003, p. 5-22.

[69] Ibid., p. 5-24.

functional cells may require a mechanism of lateral coordination to effectively synchronize their desired effects.

4. Staff Roles, Training, and Bounded Rationality

In his book *Administrative Behavior*, the prominent economist Herbert A. Simon noted "it is impossible for the behavior of a single, isolated individual to reach any high degree of rationality."[70] Simon's idea is predicated on the value information has on mental processes and how mental processes are enhanced through interpersonal exchanges.

Though Simon's work did not focus on the lateral coordination of functional units, his theory is relevant across all the information task friction points. The importance of discussing this theory emphasizes the potential interoperability friction points between functional cells independently administering information tasks.

Daily brief requirements and a communication barrage of phones and emails can easily overwhelm staff officers and focus everyone inward instead of outward. Operational and tactical level staffs need to use well-reasoned analysis, intellect, and experience to capture a commander's intent and guidance and transform them into coordinated, synchronized, resourced, and executable plans and orders. Given the increasingly complex and fluid operational environments, the Army staffs may seek shortcuts to produce

[70] Herbert Alexander Simon, *Administrative Behavior : A Study of Decision-Making Processes in Administrative Organization*, 3d ed. (New York: Free Press, 1976), pp. 79-81.

concept of operation plans rapidly, while simultaneously engaged in current operations. If enhanced lateral coordination between the information functional cells promotes information sharing and information sharing improves the synchronized application of information tasks, then the concept of lateral connectedness is not only "rational" in the Simonian sense, but a wise organizational decision.

This issue of bounded rationality leads to a number of questions regarding staff roles and training: Can the functional cells' individual staff members fluidly accomplish the new information tasks assigned to them in the 2008 FM 3-0? Do they understand the IO capabilities enough to create and oversee the execution of those information tasks? Potentially, each staff section and functional cell could view the operational environment from the perspective of their own information capabilities. Under the 2003 FM 3-0 organizational construct, no one staff section would visualize the complete information environment to determine how the information capabilities could collectively affect the means by which the adversary and civilian populations understand and use information. The lack of an information task focal point on staff could compound stove-piped planning as staff sections focus solely on their information capabilities and their segment of the operational environment.

5. Flexibility during Current Operations

While the above four friction points focused on planning, this friction point focuses on flexibility and other aspects of current operations. A staff must determine

whether an adversary commander and other targeted leaders are reacting to IO as was anticipated during planning. New adversary vulnerabilities and new information-related targets may present themselves during active military operations. Given the predominance of information systems in this century, "the time available to exploit new adversary command and control vulnerabilities may be limited and requires an immediate response" from several interdependent information elements and capabilities.[71] Flexibility is crucial to success in information task execution and staffs must be flexible enough to compensate for adversary information activities, while exploiting projected and unanticipated adversary vulnerabilities. As an operation unfolds and the operational environment becomes increasingly fluid, information objectives and tasks must be seamlessly modified to exploit success and protect friendly vulnerabilities, or risk becoming ineffectual or harmful to the mission.

6. Coordination with Higher Headquarters

IO planned and conducted by functional components must be conducted within the parameters established by higher Army headquarters or the Joint Forces Command. Subordinate services plan and execute information tasks as an integrated element of higher or Joint headquarters. The 2008 FM 3-0 is ahead of Joint doctrine which still recognizes IO as the "integrated employment" of core, supporting, and related information capabilities "to influence, disrupt, corrupt, or

[71] Department of the Army, *Field Manual 3-13, Information Operations: Doctrine, Tactics, Techniques, and Procedures,* 28 November 2003, p. 7-5.

usurp adversarial human and automated decision making while protecting our own."[72] By this definition, Joint doctrine states that IO is still the aggregate of those friendly elements that operate to influence the information dimension. The J-39 IO Cell Chief could be the higher headquarters for Army units operating under a Joint Command. This arrangement will require an Army staff information integrator that possesses a full understanding and lateral synchronization of information operations at their level, to harmonize with the Joint Planning Group. The sub-division of Army information tasks assigned to numerous staff cells could present synchronization challenges as Army units down to the tactical level of command may regularly interact with a Joint headquarters and require lateral coordination with other adjacent Services.

E. 2008 FM 3-0 LATERAL COORDINATION EVALUATION

The new 2008 FM 3-0 has dictated that the former concept of *information operations* now be divided into five Army *information tasks* in regard to the work required to operate within the information dimension of the operational environment. The responsibility for executing these information tasks has been distributed to independent staff functional cells, to arguably be synchronized through the operations process.

[72] Joint Chiefs of Staff, *Joint Publication 3-13, Information Operations,* 13 February 2006, p. ix.

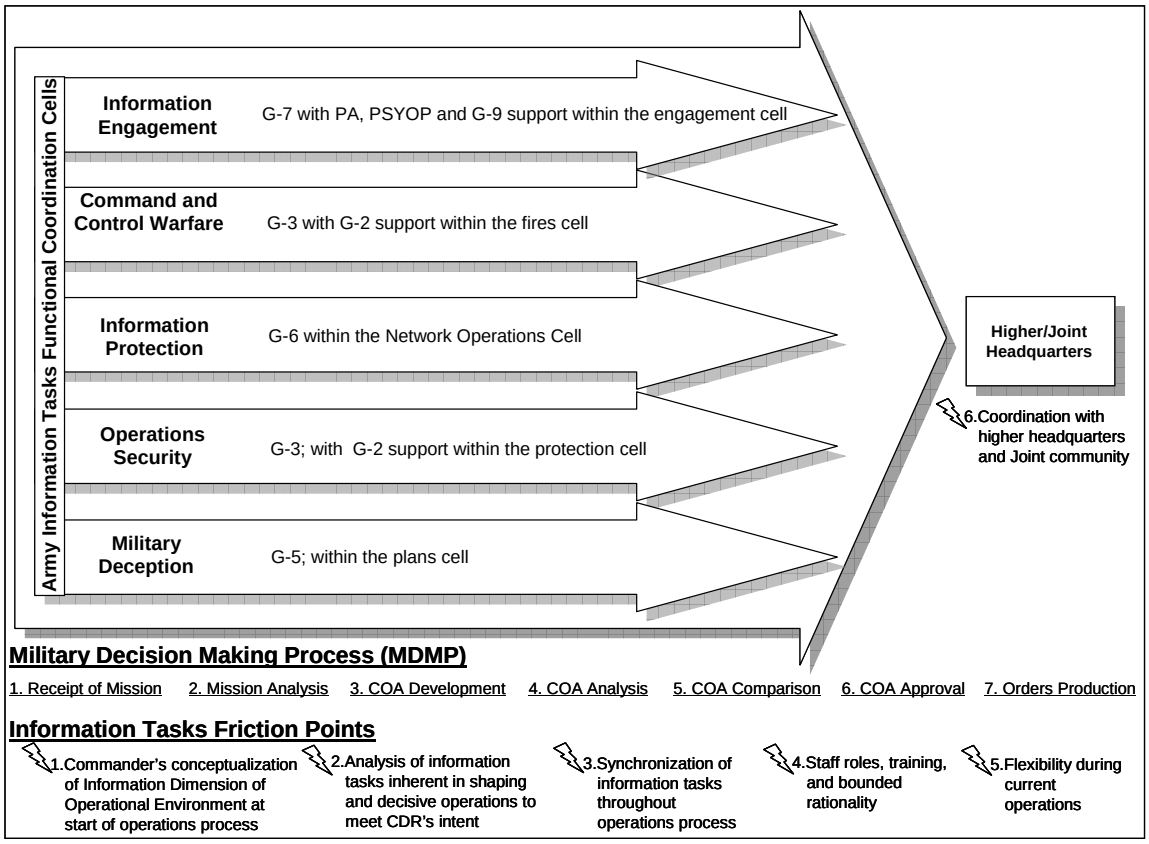

Figure 11. 2008 FM 3-0 Organizational Design.[73]

The 2008 FM 3-0 assumes that staffs will be capable of a more complex staff process and this assumption could prove risky. The *Operations* doctrine asserts that all operations should be conceived in terms of affecting human will. To synchronize the primarily cognitive information tasks, FM 3-0 suggests that the operations process, or MDMP, will be sufficient to guide the staff through the planning process and synergistic execution of the plan. Equally important, the individual information task functional cells may not be

[73] The organizational design of the 2008 FM 3-0, *Operations*, is depicted with the five delineated Information Tasks Functional Coordination Cells dealing with the six Information Tasks Friction Points throughout the Military Decision Making Process.

prepared to match higher headquarters' specified tasks with the implied informational tasks required to gain and maintain information superiority.

The Galbraith theory of lateral processes served as a structure to analyze the work to be accomplished against during planning and military operations. The six Information Tasks Friction Points exposed inherent weaknesses in the 2008 FM 3-0 organizational design's effectiveness to synchronize and accomplish informational short- and long-term goals. Without a lateral coordination process across the interdependent information functional cells, organizational effectiveness could be negatively affected and manifested through:

1. Stove-piping

Organizational theorists frequently caution against creating decentralized organizational 'silos' that lack a lateral coordination process, particularly in complex environments.[74] The self-governing information task cells could likely create boundaries that make it difficult for one functional cell to interact and synchronize information tasks with another. Each functional cell responsible for their information task risks planning the employment of their capabilities individually without knowledge of what other staff sections are planning for their information capabilities. Until the staff members laterally coordinate efforts across the doctrinal coordinating cells, there is likely to be little synergy between the information

[74] Kates and Galbraith, *Designing Your Organization : Using the Star Model to Solve 5 Critical Design Challenges*, pp. 16-17.

capabilities. Stove-piped planning without a lateral coordination mechanism could potentially result in a form of *information fratricide*, the result of employing information tasks in a way that causes effects in the information dimension that *impede* friendly military operations or adversely affect friendly forces.[75] A familiar example is friendly force electronic jamming inadvertently degrading planned PSYOP radio broadcasts.[76] Relying on an inefficient "up-across-down" flow of information in the functional cell hierarchical structure to mitigate these impediments may likely result in a loss of valuable planning time due to the unanticipated, yet required, informal synchronization and de-confliction.

2. De-synchronization

As a result of the functional cell hierarchical structure, and in the absence of mechanisms to foster coordination, the organizational structure could feasibly become a barrier to sub-unit synchronization. It is assumed that various informal coordination mechanisms will be used to overcome these barriers to promote increased sub-unit coordination and to achieve improved organizational outcomes. To accomplish this informal synchronization goal, however, each staff section responsible for information tasks would be required to attend numerous functional cell meetings at which their information capability may be discussed. Numerous coordination requirements or conflicts between capabilities could emerge at each of these

---

[75] Department of the Army, *Field Manual 3-13, Information Operations: Doctrine, Tactics, Techniques, and Procedures,* 28 November 2003, p. 1-5.

[76] Ibid., p. 1-5.

coordinating cells meetings. Each new requirement or conflict would then have to be referred back to the parent staff section to be re-planned and re-synchronized with that staff's other information capabilities, and then sent back to the coordinating cells to ensure integrated employment. The likely result would be a loss of time, redundant efforts, and reduced organizational *effectiveness*.

3. Over-reliance on an Individual

Given Simon's notion that no single individual can achieve a high degree of rationality, the expectations of the CoS and G/S-3 could prove to be unrealistic. Countless studies suggest that people differ in skills, values and beliefs. These differences often relate to ways of effective decision making in a given situation.[77]

Under the 2008 FM 3-0 information task construct, the Chief of Staff (CoS) and the G/S-3 must conduct their normal operational planning and execution duties, understand all the information capabilities and differentiate how they could affect the information dimension, and further find the time to synchronize them. The matter of over-reliance on the individual in the 2008 FM 3-0 organizational design may have less to do with the operational competency of the CoS and the G/S-3, and have more to do with *information overload* and *bounded rationality*. The problems inherent in information exceeding the individual's ability to process it, creates difficulty in determining which information is relevant.[78]

---

[77] Steven Kerr, *Organizational Behavior* (Columbus, Ohio: Grid Publishing, 1979), p. 74.

[78] Ibid., pp. 143-144.

As Mintzberg has shown, successful management is impeded by time pressures and competition between wide varieties of tasks.[79] Without a lateral information task coordinator, the CoS or the G/S-3 task manager will be required to nominate, synchronize, and de-conflict information capabilities while simultaneously performing their extensive doctrinal operational duties.

4. Incompatibility

Information tasks planned and conducted by subordinate units assigned to a Joint headquarters must be conducted within the parameters established by the Joint Forces Commander. Joint headquarters plan and synchronize information operations through the J-39 IO Cell Chief. A primary function of the J-39 is to ensure that IO are 'integrated and synchronized in all planning processes' and that IO are coordinated with subordinate staffs.[80] Components are responsible for the detailed planning and execution of IO, yet the Army component must conduct these information activities within the parameters established by the Joint Force Commander. With no corresponding information coordinator at the Army headquarters, this could create friction between the Joint task force and the Army service component.

To integrate and synchronize the *core*, *supporting*, and *related* capabilities of IO, the J-39 normally leads an *IO Cell* as an integrated component of the staff's operational

---

[79] Henry Mintzberg, *The Structuring of Organizations: A Synthesis of the Research* (Englewood Cliffs, N.J.: Prentice-Hall, 1979), pp. 24-29.

[80] Joint Chiefs of Staff, *Joint Publication 3-13, Information Operations,* 13 February 2006, p. xiii.

planning group.[81] The organizational relationship between the joint IO Cell and the Army service component could become strained, as multiple subordinate Army staff sections would have to coordinate directly with the J-39. More seriously yet, Army corps or divisions serving as a Joint Task Force will either have to create a J-39 or have each of their staff sections responsible for an individual Army information task coordinate directly with the information operations staffs at Air Force, Navy and Marine Corps subordinate headquarters. While this information task friction point seems to be centered on echelons above the scope of this research, only the complexity and length of planning horizons differ at the operational and tactical levels, and IO execution complexity stems from the multiple information elements and the coordination required between echelons.

F. CONCLUSION

This chapter built upon previously introduced guidelines of how the U.S. Army accomplishes information tasks at the operational and tactical levels of warfare and planning. By identifying information friction points, the evaluation of the 2008 FM 3-0 organizational design indicated that the functional structure of the Army interdependent information task cells could become a barrier as it becomes necessary to synchronize and de-conflict their activities across other cells. Assuming this hypothesis is true, the 2008 FM 3-0 organizational design of five

[81] Joint Chiefs of Staff, *Joint Publication 3-13, Information Operations,* 13 February 2006, p. xiii.

independent functional cells could create negative friction points that reduces optimal functionality.

By all indications, the proposition of a lateral coordination mechanism does not violate the general organizational guidance found in FM 3-0. Just as commanders are given the latitude to "match information tasks with actions on the ground,"[82] they are also allowed the flexibility to organize their staffs when dealing with specific tactical and operational situations. The aim of the 2008 FM 3-0 is to establish guidelines for leaders to direct operations while allowing enough freedom for bold, creative initiative in any situation. While the codification of a formal lateral coordination mechanism synchronizing the information task coordination cells may not invoke creative initiative, it does establish a logical framework to mitigate information task friction points inherent in planning and conducting military operations.

[82] Department of the Army, *Field Manual 3-0, Operations,* 27 February 2008, p. 7-2.

V. RECOMMENDATIONS

This chapter contains observations from the lateral processes analysis and provides recommendations for the Army operational and tactical organizations executing information tasks. Given the determination in the previous chapter of how the various information functional cells will be required to interact to achieve the output goal, it is now necessary to illustrate how a formal lateral coordination device between the cells could mitigate the negative effects of the information friction points.

Organizational contingency theory is founded on two chief principles.[83] The first principle is that there is no one best way to organize. The suitability of an organization's structural arrangement relies on a number of factors. These factors can, for example, be the level of complexity and uncertainty in the operational environment. The second principle is that all ways of organizing are not equally effective. Specifically, organizations that demonstrate structures that fit the requirements of their environment will be more effective than organizations which do not.[84]

An informed judgment can now be made regarding the benefit of lateral coordination between the information functional cells. First, it was determined that the 2008 FM 3-0 organizational design of five independent functional

---

[83] Galbraith, *Designing Complex Organizations*, p. 2.

[84] Richard M. Burton and Børge Obel, *Strategic Organizational Diagnosis and Design: Developing Theory for Application*, 2nd ed. (Boston: Kluwer Academic Publishers, 1998), pp. 15-18.

cells could create negative friction points that reduces optimal functionality. Assuming that this analysis is true, the second issue to be resolved is whether a formal lateral coordination device between the cells could mitigate the negative friction points, thus, aiding in synergistically accomplishing information tasks in a complex operating environment.

A. 2001 FM 3-0 AND 2008 FM 3-0 HYBRID ORGANIZATIONAL DESIGN

My hypothesis is that a hybrid of the 2008 FM 3-0 organizational design and its 2001 predecessor's design will best synchronize the accomplishment of the interdependent information tasks, producing a structural arrangement that will be most effective in incorporating information tasks into the complex operational environment. The suggested hybrid cannot, however, violate the 2008 FM 3-0 as it is approved doctrine. The 2001 FM 3-0, *Operations*, and the 2003 FM 3-13, *Information Operations*, mandated that it was the role of the G/S-7 to assist the commander's understanding of the information dimension of the operating environment at the beginning, and throughout the MDMP. As a trained staff officer in the employment of the core, supporting and related information capabilities, the G/S-7 was the accountable staff principle who synchronized information activities derived from knowledge and expertise of the full range of IO capabilities and related activities.

B. HYBRID DESIGN LATERAL COORDINATION

The dictated alignment of information tasks to the responsible staff element is based on sound reasoning.

Affecting the Information Dimension requires a combined staff effort in a combined arms approach. There is but one *operational environment*, and physical maneuver operations, words, and images directed at any aspect of the operational environment affects the information dimension.[85] While this research does not question the reasoning for aligning information task responsibility with the staff proponents possessing the deepest knowledge of the capabilities and intended effects, it does assert that the organizational effectiveness in accomplishment of Army Information Tasks can be improved by establishing a lateral coordination mechanism to increase lateral control.

By establishing a lateral coordination liaison or full-time integrator, the recognized Information Task Friction Points can be mitigated along the MDMP and throughout the conduct of operations. During the MDMP, critical informational dimension requirements present themselves that require identifying, analyzing, and understanding of those publics and actors whose perceptions, attitudes, beliefs, and behaviors will affect the unit's mission.

[85] Department of the Army, *Field Manual 3-0, Operations,* 27 February 2008, p. 1-1.

Information Tasks Friction Points	Lateral coordination Liaison or full-time Integrator mitigation
1. Commander's conceptualization of the Information Dimension of the Operational Environment at start of the operations process (MDMP)	Coordinator assists the commander's understanding of the Information Dimension through the Staff Estimate process
2. Analysis of information tasks inherent in shaping and decisive operations to meet Commander's Intent	Coordinator has coordinating staff responsibility for IO with support in the IO and Fires Cells
3. Synchronization of information tasks throughout operations process	Coordinator's primary function is to synchronize IO throughout the operations process
4. Staff roles, training, and bounded rationality	Coordinator identifies IO targets and nominates them through the Targeting process
5. Flexibility during current operations	Coordinator estimates the effectiveness of IO task execution, adjusting to a changing friendly situation or adversary reaction
6. Coordination with Higher Headquarters and Joint community	Coordinator synchronizes IO objectives/tasks with counterparts at higher and Joint echelons

Table 2. Lateral Coordinator affect on Information Tasks Friction Points.[86]

The lateral processes analysis concluded that there is a need for an Army information task coordinator to manage the coordination of the information tasks into operational planning and execution. In addition, the analysis showed how the staff alignment of the Army information tasks could be enhanced and friction points mitigated by a lateral coordination mechanism with the responsibility for synchronizing the Army staff's information tasks through:

1. Direct Liaison

The first method to achieve lateral coordination among the interdependent Army information functional cells is to create a duty position within the G/S-3 for a trained,

[86] Information Tasks Friction Points mitigated by a formal lateral coordination role.

certified, and qualified information task coordinator to liaise across all of the functional information cells. The G/S-3 could assign this liaison officer from his section to bridge the functional cells in order to synchronize information tasks, or the G/S-7 could serve this function on behalf of the G/S-3 while simultaneously serving as a member of the *Information Engagement* functional cell.

The information task liaison would be responsible for coordination and synchronization of the information tasks functional coordination cells to insure information capabilities are correctly applied and no unintentional information effects occur. The role of the liaison is not intended as a reversion back to the concept of the G/S-7 as codified in the 2001 FM 3-0 and 2003 FM 3-13. *Coordination* was the role originally intended of the Information Operations Officer, yet organizational uncertainty led to the misperception that the G/S-7 was responsible for executing the numerous *core* and *supporting* elements of IO. With an information tasks liaison mechanism in place, the information task functional cells would still remain responsible for accomplishment of the information tasks, while the liaison is given the responsibility for synchronization, troubleshooting, and conflict resolution.

2. Full-time Integrator

Another method to achieve an even greater lateral control between the information functional cells is to establish a fully trained, certified and qualified information capabilities integrator duty position to administer the work of the five information functional cells. The role of the staff information capabilities

integrator would be to match the *core*, *supporting*, and *related* information operations capabilities with each functional cell's information requirements, then coordinate and synchronize the information tasks across those cells.

This lateral control mechanism again requires the creation of a duty position within the G/S-3 of a trained, certified and qualified information task coordinator to integrate the functional cells, or involves empowering the G/S-7 to achieve this integration function while participating as a member of the *Information Engagement* functional cell. An integration role provides a higher level of coordination than the direct liaison and the information task integrator would have accountability for information task accomplishment, but not directly manage the resources required to achieve those results.

The integrator achieves this power through a direct reporting relationship to the commander. The 2001 FM 3-0 and 2003 FM 3-13 stipulated that the G/S-7s were responsible for coordinating all IO capabilities. In this respect, G/S-7s were considered *integrators* of IO capabilities and the accountable staff principal who synchronized information activities derived from his training, knowledge, and expertise of IO capabilities and related activities. The difference between the 2001 FM 3-0 paradigm and the information tasks integrator concept includes a higher degree of lateral control in the latter. The assigned G/S-3 integrator or the G/S-7 would directly administer the work of the five information functional cells, and assume responsibility for accomplishment of the information tasks. In order to mitigate the information friction points

encountered during the MDMP and the execution of operations, the integrator would increase the effectiveness of the staff's information task accomplishment by:

- Assisting the commander's understanding of the Information Dimension through the Staff Estimate process.
- Coordinating staff responsibility for IO with support in the IO and Fires Cells.
- Synchronizing IO throughout the operations process.
- Identifying IO targets and nominates them through the targeting process.
- Estimating the effectiveness of IO task execution, adjusting to a changing friendly situation or adversary reaction.
- Synchronizing IO objectives and necessary information tasks with counterparts at higher and Joint echelons.

The interdependent nature of the tasks of the Army information functional cells requires either a liaison or an integrator form of lateral coordination across those cells. The 2008 FM 3-0 organizational restructuring was intended to increase the staffs' understanding of the information dimension's impact on the operational environment. The proposed addition of an information task coordinator further enhances the effectiveness of the staff as it develops information tasks and integrates them into full spectrum operations as synergistically as it had the other elements of combat power, such as fires, maneuver, protection and sustainment.

C. CONCLUSION

The first phase of this study identified the five Army information tasks, with the responsibility redistributed to different staff functional cells, ultimately to be synchronized by the operations process. Descriptions of each coordination cell and each of their information capabilities were explained and information friction points were identified to illustrate symptoms of desynchronized information operations that negatively affect military operations.

The second phase of this study demonstrated how the 2008 FM 3-0 organizational design lacked a sufficient degree of effectiveness to laterally coordinate the *reciprocally interdependent* information tasks. Observations from the lateral processes analysis led to subsequent recommendations for more effectively organizing Army operational and tactical units executing information tasks.

This study contends that a hybrid of the 2008 FM 3-0 organizational design and its 2001 predecessor's design will best synchronize the accomplishment of the interdependent information tasks, producing a structural arrangement that will be most effective in incorporating information tasks into the complex operational environment. There is a need for a formal information tasks coordinator to oversee the synchronization of the information tasks into operational planning and execution, and this function can be achieved by appointing a G/S-3 or G/S-7 liaison officer or full-integrator to accomplish the required degree of lateral coordination. In short, the combined performance and effectiveness of the operational and tactical Army staff

organization requires this lateral process of coordination to synchronize the highly-interdependent information tasks.

Information is elemental to combat power, but to properly and effectively employ this capability requires coordination, synchronization, and integration with the other warfighting elements. As FM 3-0 asserts, “commanders must understand [information], integrating it in full spectrum operations as carefully as fires, maneuver, protection, and sustainment.”[87] To comply with this mandate, commanders require a lateral coordinator whose dual-role or sole mission focus is to synchronize the Army information tasks and the information capabilities within those tasks.

[87] Department of the Army, *Field Manual 3-0, Operations,* 27 February 2008, p. 7-1.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX – ARMY INFORMATION TASKS FUNCTIONAL COORDINATION CELLS STAFFING

This Appendix will discuss the execution of the five IO tasks by the individual proponents and capabilities in each of the responsible functional coordination cells as codified in the 2008 FM 3-0.

A. INFORMATION ENGAGEMENT FUNCTIONAL COORDINATION CELL

The primary staff responsibility for the conduct of the Information Engagement functional cell is the G/S-7 Information Operations Officer with Public Affairs, PSYOP and G/S-9 Civil Affairs support within the information engagement cell. The staff proponents and capabilities of the Information Engagement Cell include:

1. Leader and Soldier Engagement

Soldiers' actions are the most powerful component of information engagement. Visible actions coordinated with carefully chosen, truthful words influence audiences more than either does alone. Face-to-face interaction by leaders and soldiers strongly influences the perceptions of the local populace. Carried out with discipline and professionalism, day-to-day interaction of Soldiers with the local populace among whom they operate can have positive effects.

As the primary staff responsibility for the conduct of the Information Engagement functional cell, G/S-7s serve as the Commander's focal point for achieving the full potential

of information, engagement, communication, and collaboration in an era of persistent conflict. Specifically, they may:

- Coordinate the information engagement activities and ensure the proper integration of those activities into base plans and orders.
- Assist in identifying, analyzing, and understanding those publics and actors whose perceptions, attitudes, beliefs, and behaviors affect the unit's mission.
- Assist in determining the desired end state conditions for each relevant public and actor in terms of perceptions, attitudes, beliefs, and behavior.
- Assist with the campaign design, ensuring planned deeds, words, and images are mutually reinforcing and likely to produce the intended change in behavior.
- Assist in developing a campaign or mission narrative.[88]

2. Public Affairs

Public Affairs (PA) is defined as '*Those public information, command information, and community relations activities directed toward both the external and internal publics with interest in the Department of Defense*.'[89] Public Affairs forms an important part in the dissemination of truthful information to both internal and external audiences so that a correct perspective of combat operations is projected. A more coordinated and deliberate approach is required to match the actions on the ground with what is

---

[88] U.S. Army Information Operations Proponent, U.S. Army Combined Arms Center, *Fact Sheet: Functional Area 30 Qualification Course (FA30 QC),* 15 October 2008.

[89] Joint Chiefs of Staff, *Joint Publication 1-02, DOD Dictionary of Military and Associated Terms,* 12 April 2001, as Amended through 30 May 2008, p. 442.

projected through PA outlets. It is also used to counter adversaries' misinformation and disinformation campaigns through dissemination of accurate information.

3. Psychological Operations

PSYOP are defined as '*Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of PSYOP is to induce or reinforce foreign attitudes and behavior favorable to the originator's objective*.'[90] The PSYOP objectives are met through the use of radio, print, and other electronic media. The cross-cultural and regional understanding for conducting successful PSYOP against target audiences is an essential element.

4. Combat Camera

Combat Camera (COMCAM) is defined as '*The acquisition and utilization of still and motion imagery in support of combat, information, humanitarian, intelligence, reconnaissance, engineering, legal, public affairs, and other operations involving the Military Services*.'[91] COMCAM is effectively used for the battle of ideas and provides the imagery requirement for PSYOP, MILDEC, PA and CMO. COMCAM products can also be disseminated to regional media organizations to achieve wider publicity and for use in

---

[90] Joint Chiefs of Staff, *Joint Publication 1-02, DOD Dictionary of Military and Associated Terms,* 12 April 2001, as Amended through 30 May 2008, p. 441.

[91] Ibid., p. 97.

subtle influence operations toward a wider public audience. The dissemination of such products may also be conducted through the Internet so as to exploit the reach of the Internet in news or imagery propagation.

5. Strategic Communication and Defense Support to Public Diplomacy

Strategic Communication is defined as '*Focused United States Government efforts to understand and engage key audiences to create, strengthen, or preserve conditions favorable for the advancement of United States Government interests, policies, and objectives through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all instruments of national power*.'[92]

Defense Support to Public Diplomacy (DSPD) is defined by the U.S. military as '*Those activities and measures taken by the Department of Defense components to support and facilitate public diplomacy efforts of the United States Government*.'[93] This activity is conducted at the strategic and operational level and attempts to mesh the foreign policy objectives with much broader goals including specific military information operations objectives. The operations conducted by the Army at the tactical level also fall into this category since they can either support the overall public diplomacy effort or cause an adverse impact. The vulnerability of military field operations to cause an

---

[92] Joint Chiefs of Staff, *Joint Publication 1-02, DOD Dictionary of Military and Associated Terms,* 12 April 2001, as Amended through 30 May 2008, p. 522.

[93] Ibid., p. 150.

adverse impact on the information dimension of the operational environment needs to be adequately factored and duly understood by military commanders at all levels.

B. COMMAND AND CONTROL WARFARE FUNCTIONAL COORDINATION CELL

The primary staff responsibility for the conduct of the Command and Control Warfare functional cell is the G/S-3 Operations Officer with G/S-2 Intelligence Officer support within the fires cell. The staff proponents and capabilities of the Command and Control Warfare Cell include:

1. Physical Attack

Physical attack disrupts, damages, or destroys adversary targets through the use of destructive power, and is fundamental to all military operations. It may lead to create or alter adversary perceptions or to facilitate an adversary to use certain exploitable information systems. In terms of a supporting element of information operations, it needs to be integrated with PSYOP to achieve the required influence over a target audience and coordinated to destroy specific command and control nodes of the adversary. This facet allows synchronization between the physical objectives and the informational objectives in a battlefield.

2. Electronic Warfare (minus Electronic Protection)

Electronic Warfare (EW) is defined as '*Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the*

enemy.'[94] EW includes three major sub-divisions: electronic protection (EP), which is a component of the Information Protection Functional Coordination Cell, **electronic attack (EA)**, 'Involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires,'[95] and **electronic warfare support (ES)**, 'Involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations.'[96] ES is utilized to monitor, identify, locate, and derive actionable intelligence about adversaries through the use of electromagnetic sensors, both in the communication and non-communication bands. EA is more is terms of denying the use of the electromagnetic spectrum to adversaries for their communication and control.

3. Computer Network Operations (minus Computer Network Defense)

Computer Network Operations (CNO) are described as operations to *attack, deceive, degrade, disrupt, deny, exploit, and defend electronic information and*

---

[94] Joint Chiefs of Staff, *Joint Publication 1-02, DOD Dictionary of Military and Associated Terms,* 12 April 2001, as Amended through 30 May 2008, p. 180.

[95] Ibid., pp. 178-179.

[96] Ibid., p. 180.

infrastructure. CNO is divided into three major components: computer network defense (CND), which is a component of the *Information Protection Functional Coordination Cell*, **computer network attack (CNA)**, *'Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves,'*[97] and **computer network exploitation (CNE)**, *'Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.'*[98] CNA is comprised of all destructive and disruptive actions, while CNE involves enabling operations and intelligence collection capabilities through the use of networks and information systems. The information in today's information age resides on information systems and flows on the information networks. The ability to regulate information on closed systems is still an achievable action, but regulation of the same on global open systems like the Internet is almost impossible in the present context.

C. INFORMATION PROTECTION FUNCTIONAL COORDINATION CELL

The primary staff responsibility for the conduct of the Information Protection functional cell is the G/S-6 Communications Officer within the Network Operations Cell. The staff proponents and capabilities of the Information Protection Cell include:

---

[97] Joint Chiefs of Staff, *Joint Publication 1-02, DOD Dictionary of Military and Associated Terms,* 12 April 2001, as Amended through 30 May 2008, p. 112.

[98] Ibid., p. 112.

1. Information Assurance

Information Assurance (IA) is defined as '*Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities*.' IA is part of the defensive mechanism necessary for protection of information systems.

2. Computer Network Defense

As part of Computer Network Operations (CNO), Computer Network Defense (CND) involves '*Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks*.'[99]

The military information infrastructure is vulnerable to actions by terrorists largely due to the target size involved, as well as a triggering-effect that may be caused by an action and its flow on interconnected global networks; CND, therefore, assumes considerable significance.

3. Electronic Protection

Electronic Protection (EP) is the '*Division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of*

[99] Joint Chiefs of Staff, *Joint Publication 1-02, DOD Dictionary of Military and Associated Terms,* 12 April 2001, as Amended through 30 May 2008, p. 112.

friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability.'[100]

D. OPERATIONS SECURITY FUNCTIONAL COORDINATION CELL

The primary staff responsibility for the conduct of the Operations Security functional cell is the G/S-3 Operations Officer with G/S-2 Intelligence Officer support within the protection cell. The staff proponents and capabilities of the Operations Security Cell include:

1. Operations Security

Operations Security (OPSEC) is defined as '*A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. identify those actions that can be observed by adversary intelligence systems; b. determine indicators that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and c. select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation*.'[101]

2. Physical Security

Physical security is defined as '*That part of security concerned with physical measures designed to safeguard*

---

[100] Joint Chiefs of Staff, *Joint Publication 1-02, DOD Dictionary of Military and Associated Terms,* 12 April 2001, as Amended through 30 May 2008, p. 179.

[101] Ibid., p. 401.

personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft.' Physical security contributes towards OPSEC and MILDEC.

3. Counterintelligence

Counterintelligence (CI) is defined as '*Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities*.'[102] Counterintelligence is an essential element of antiterrorism and counterterrorism procedures and forms part of both defensive and offensive measures against terrorist organizations and networks.

E. MILITARY DECEPTION FUNCTIONAL COORDINATION CELL

The primary staff responsibility for the conduct of the Military Deception functional cell is the G/S-5 Plans Officer within the plans cell. The staff proponents and capabilities of the Military Deception Cell could include a cross-section of the entire staff, as MILDEC operations are planned and subjected to the same operations process as legitimate operations.

---

[102] Joint Chiefs of Staff, *Joint Publication 1-02, DOD Dictionary of Military and Associated Terms,* 12 April 2001, as Amended through 30 May 2008, p. 129.

1. Military Deception

Military Deception (MILDEC) is defined as *'Actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission.'*[103]

MILDEC in the information domain is quite different from the traditional or conventional MILDEC that involved the fusing of deception with physical tangibles on the ground; in the information age, MILDEC may achieve success by shaping the information without too much reliance on commensurate actions in the physical domain. This ability to move away from traditional employment of MILDEC will truly allow it to be integrated in information operation campaigns against terrorist organizations and networks. The importance of understanding the adversary's *'collection systems and sensors,'* to absorb deception, and to correctly assess their attitudes and reactions, is an essential ingredient for a successful MILDEC operation.

F. CIVIL-MILITARY OPERATIONS

Civil-Military Operations is conspicuously omitted as a member of its sensible position in the Information Engagement Cell, the cell charged with "influencing foreign audiences." This omission has not been explained in the doctrine or otherwise. Civil-Military Operations (CMO) are

---

[103] Joint Chiefs of Staff, *Joint Publication 1-02, DOD Dictionary of Military and Associated Terms,* 12 April 2001, as Amended through 30 May 2008, p. 341.

defined as *'The activities of a commander that establish, maintain, influence, or exploit relations between military forces, governmental and nongovernmental civilian organizations and authorities, and the civilian populace in a friendly, neutral, or hostile operational area in order to facilitate military operations, to consolidate and achieve operational US objectives.'*[104] Civil-Military Operations are conducted across the range of military operations over all phases - starting from the preparatory phase, through to the stabilization and reconstruction phase.

[104] Joint Chiefs of Staff, *Joint Publication 1-02, DOD Dictionary of Military and Associated Terms,* 12 April 2001, as Amended through 30 May 2008, p. 89.

LIST OF REFERENCES

Baker, Ralph O. “The Decisive Weapon: A Brigade Combat Team Commander’s Perspective on Information Operations.” *Military Review* (May-June, 2006), http://www.army.mil/professionalwriting/volumes/volume4/july_2006/7_06_3.html (accessed 6/17/2008).

Burton, Richard M. and Børge Obel. *Strategic Organizational Diagnosis and Design: Developing Theory for Application*. 2nd ed. (Boston: Kluwer Academic Publishers, 1998).

Combined Arms Doctrine Directorate (CADD). *Army Doctrine Update,* 24 February 2007. (Fort Leavenworth, Kansas: US Army Combined Arms Center, 2007), http://asc.army.mil/docs/transformation/Army_Doctrine_Update_FM501_FM30.pdf (accessed 8/20/08).

Daft, Richard L. and Raymond A. Noe. *Organizational Behavior*. (Mason, OH: South-Western, 2001).

Department of the Army. *Field Manual 3-0, Operations,* 27 February 2008. (Washington, D.C.: Headquarters, Department of the Army, 2008), https://akocomm.us.army.mil/usapa/doctrine/DR_pubs/dr_aa/pdf/fm3_0.pdf (accessed 5/15/08).

———. *Field Manual 5-0, Army Planning and Orders Production, Dtd.* 20 January 2005. (Washington, D.C.: Headquarters, Department of the Army, 2005), https://akocomm.us.army.mil/usapa/doctrine/DR_pubs/dr_aa/pdf/fm5_0.pdf (accessed 5/16/08).

———. *Field Manual 1-02, Operational Terms and Graphics,* 21 September 2004. (Washington, D.C.: Headquarters, Department of the Army, 2004), https://akocomm.us.army.mil/usapa/doctrine/DR_pubs/dr_aa/pdf/fm1_02.pdf (accessed 5/21/08).

———. *Field Manual 3-13, Information Operations: Doctrine, Tactics, Techniques, and Procedures,* 28 November 2003. (Washington, D.C.: Headquarters, Department of the Army, 2003), https://akocomm.us.army.mil/usapa/doctrine/DR_pubs/dr_aa/pdf/fm3_13.pdf (accessed 5/16/08).

———. *Field Manual 6-0, Mission Command: Command and Control of Army Forces,* 11 August 2003. (Washington, D.C.: Headquarters, Department of the Army, 2003), https://akocomm.us.army.mil/usapa/doctrine/DR_pubs/dr_aa/pdf/fm6.pdf (accessed 8/14/08).

———. *Field Manual 100-6, Information Operations,* 27 August 1996. (Washington, D.C.: Headquarters, Department of the Army, 1996), http://www.iwar.org.uk/iwar/resources/usarmyio/fm100-6.pdf (accessed 5/16/08).

Department of the Army, Office of the Deputy Chief of Staff, G8. *2007 Army Modernization Plan*. (Washington D.C.: Office of the Deputy Chief of Staff, G8, 2007), http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=ADA468000&Location=U2&doc=GetTRDoc.pdf (accessed 8/20/08).

Galbraith, Jay R. *Designing Organizations : An Executive Guide to Strategy, Structure and Process*. The Jossey-Bass Business & Management Series. New and rev. ed. (San Francisco: Jossey-Bass, 2002).

———. *Designing Complex Organizations*. Addison-Wesley Series on Organization Development. (Reading, Mass.: Addison-Wesley Pub. Co, 1973).

Galbraith, Jay R., Diane Downey, and Amy Kates. *Designing Dynamic Organizations*. (New York: Amacom, 2002).

Herbert, Paul H. and U.S. Army Command and General Staff College. Combat Studies Institute. *Deciding what has to be done: General William E. DePuy and the 1976 Edition of FM 100-5, Operations*. Leavenworth Papers. Vol. 16. (Fort Leavenworth, Kan.: Combat Studies Institute, U.S. Army Command and General Staff College, 1988), http://www-cgsc.army.mil/carl/resources/csi/Herbert/Herbert.asp#3 (accessed 16/8/08).

Joint Chiefs of Staff. *Joint Publication 3-0, Joint Operations,* 17 September 2006, Change 1, 13 February 2008. (Washington, D.C.: Joint Staff, 2006), http://www.dtic.mil/doctrine/jel/new_pubs/jp3_0.pdf (accessed 2/24/08).

———. *Joint Publication 3-13, Information Operations,* February 13, 2006. (Washington, D.C.: Joint Staff, 2006), http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf (accessed 3/6/08).

———. *Chairman of the Joint Chiefs of Staff Manual CJCSM 3500.04C, Universal Joint Task List (UJTL),* July 1 2002. (Washington, D.C.: Joint Staff, 2002), http://www.dtic.mil/doctrine/jel/cjcsd/cjcsm/m350004c.pdf (accessed 3/03/08).

———. *Joint Publication 1-02, DOD Dictionary of Military and Associated Terms,* 12 April 2001, as Amended through 30 May 2008. (Washington, D.C.: Joint Staff, 2001), http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf (accessed 4/23/08).

Kates, Amy and Jay R. Galbraith. *Designing Your Organization : Using the Star Model to Solve 5 Critical Design Challenges*. 1st ed. (San Francisco: Jossey-Bass, 2007).

Kerr, Steven. *Organizational Behavior*. The Grid Series in Management. (Columbus, Ohio: Grid Publishing, 1979).

Mintzberg, Henry. *The Structuring of Organizations: A Synthesis of the Research*. (Englewood Cliffs, N.J.: Prentice-Hall, 1979).

Paparone, Christopher R. “US Army Decisionmaking: Past, Present and Future.” *Military Review* (July-August, 2001).

Romanych, Marc J. “Tactical Information Operations in Kosovo.” *Military Review* (September-October, 2004), www.au.af.mil/au/awc/awcgate/milreview/romanych.pdf (accessed 6/17/2008).

Simon, Herbert Alexander. *Administrative Behavior : A Study of Decision-Making Processes in Administrative Organization*. 3d ed. (New York: Free Press, 1976).

Snook, Scott A. *Friendly Fire : The Accidental Shootdown of U.S. Black Hawks Over Northern Iraq*. (Princeton, N.J.: Princeton University Press, 2000).

Thompson, James D. *Organizations in Action: Social Science Bases of Administrative Theory*. (New York: McGraw-Hill, 1967).

U.S. Army Information Operations Proponent, U.S. Army Combined Arms Center. *Fact Sheet: Functional Area 30 Qualification Course (FA30 QC),* 15 October 2008. (Fort Leavenworth, Kansas: U.S. Army Combined Arms Center, 2008).

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dr. Hy Rothstein
   Department of Defense Analysis
   Naval Postgraduate School
   Monterey, California

4. Dr. Erik Jansen
   Department of Information Sciences
   Naval Postgraduate School
   Monterey, California

5. Jennifer Duncan
   Department of Defense Analysis
   Naval Postgraduate School
   Monterey, California