THE INFORMATION OPERATIONS COORDINATION CELL—NECESSARY FOR DIVISION OFFENSIVE ACTIONS?

A MONOGRAPH
BY
Major Rosemary M. Carter
Signal Corps

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas

First Term AY 98-99

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	16 DECEMBER 1998	MONOGRAPH

4. TITLE AND SUBTITLE
THE INFORMATION OPERATIONS COORDINATION CELL—NECESSARY FOR DIVISION OFFENSIVE ACTIONS?

5. FUNDING NUMBERS

6. AUTHOR(S)
MAJOR ROSEMARY M. CARTER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
SCHOOL OF ADVANCED MILITARY STUDIES
COMMAND AND GENERAL STAFF COLLEGE
FORT LEAVENWORTH, KANSAS 66027

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
COMMAND AND GENERAL STAFF COLLEGE
FORT LEAVENWOATH, KANSAS 66027

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

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

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)
SEE ATTACHED

14. SUBJECT TERMS
INFORMATION OPERATIONS
OPERATIONAL SECURITY
PSYCHOLOGICAL OPERATIONS
ELECTRONIC WARFARE
MILITARY DECEPTION

15. NUMBER OF PAGES
58

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

ABSTRACT

THE INFORMATION OPERATIONS COORDINATION CELL - NECESSARY FOR DIVISION OFFENSIVE ACTIONS? by MAJ Rosemary M. Carter, USA, 48 pages

This monograph analyzes the need for a division Information Operations (IO) Coordination Cell during offensive military actions.

The integrated concept team draft of FM 100-6, Information Operations: Tactics, Techniques and Procedures, includes a division Information Operations Coordination Cell. The cell is responsible for integrating the components of Information Superiority (IS) to defeat the enemy's command, control, computers, communications, intelligence, surveillance and reconnaissance (C4ISR) while protecting friendly C4ISR. Their focus is the Information Operations segment of IS that includes operational security (OPSEC), psychological operations (PSYOP), military deception, electronic warfare (EW), physical destruction, computer network attack (CNA), public affairs (PA), and civil affairs (CA).

The monograph restricts the topic to Offensive IO, or IO that attacks the enemy commander's ability to achieve his objectives. Also, the monograph limits the type of military action to offensive. The current draft of FM 100-5, Operations, dated June 1998 divides operations into four types of military actions - offense, defense, stability and support. The monograph focuses on offensive actions, the primary action within offensive operations, because that is what the Army is designed for - fighting and winning wars.

The monograph analyzes the IO tasks using three supporting research processes. First, it determines that only five of the tasks are necessary for Offensive IO - PSYOP, military deception, EW, physical destruction, and CA. The monograph then analyzes current doctrine and the heavy division Army of Excellence Table of Organization and Equipment (TOE) to determine the division's capabilities to execute the Offensive IO tasks. Finally, the monograph uses these capabilities and doctrine to determine if the current division staff has the necessary staff mechanisms to conduct the Offensive IO tasks. The monograph determines that the proper staff mechanisms are in place to conduct the Offensive IO tasks that the division has the capability to execute.

As a final inquiry, the monograph analyzes the IO staff responsibilities outlined in the draft FM 100-6. The monograph identifies two tasks, establish and publish Offensive IO priorities, and battletrack Offensive IO, that were not assigned IO tasks. The monograph concludes that to conduct these tasks the division does not need a separate six soldier IO Coordination Cell, but rather one officer functioning much like the current FSCOORD or SOCOORD.

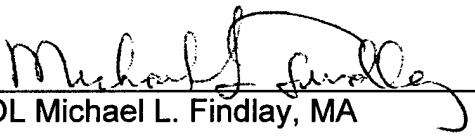
SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

Major Rosemary M. Carter

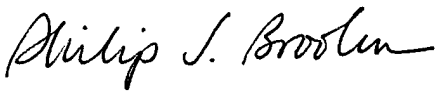
Title of Monograph: *The Information Operations Coordination Cell – Necessary for Division Offensive Actions?*

Approved by:



COL Michael L. Findlay, MA — Monograph Director

LTC Robin P. Swan, MMAS — Director, School of Advanced Military Studies



Philip J. Brookes, Ph.D. — Director, Graduate Degree Program

Accepted this 16th Day of December 1998

The Information Operations Coordination Cell - Necessary for Division Offensive Actions?

A Monograph
By
Major Rosemary M. Carter
Signal Corps

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas

First Term AY 98-99

ABSTRACT

THE INFORMATION OPERATIONS COORDINATION CELL - NECESSARY FOR DIVISION OFFENSIVE ACTIONS? by MAJ Rosemary M. Carter, USA, 48 pages

This monograph analyzes the need for a division Information Operations (IO) Coordination Cell during offensive military actions.

The integrated concept team draft of FM 100-6, Information Operations: Tactics, Techniques and Procedures, includes a division Information Operations Coordination Cell. The cell is responsible for integrating the components of Information Superiority (IS) to defeat the enemy's command, control, computers, communications, intelligence, surveillance and reconnaissance (C4ISR) while protecting friendly C4ISR. Their focus is the Information Operations segment of IS that includes operational security (OPSEC), psychological operations (PSYOP), military deception, electronic warfare (EW), physical destruction, computer network attack (CNA), public affairs (PA), and civil affairs (CA).

The monograph restricts the topic to Offensive IO, or IO that attacks the enemy commander's ability to achieve his objectives. Also, the monograph limits the type of military action to offensive. The current draft of FM 100-5, Operations, dated June 1998 divides operations into four types of military actions - offense, defense, stability and support. The monograph focuses on offensive actions, the primary action within offensive operations, because that is what the Army is designed for - fighting and winning wars.

The monograph analyzes the IO tasks using three supporting research processes. First, it determines that only five of the tasks are necessary for Offensive IO - PSYOP, military deception, EW, physical destruction, and CA. The monograph then analyzes current doctrine and the heavy division Army of Excellence Table of Organization and Equipment (TOE) to determine the division's capabilities to execute the Offensive IO tasks. Finally, the monograph uses these capabilities and doctrine to determine if the current division staff has the necessary staff mechanisms to conduct the Offensive IO tasks. The monograph determines that the proper staff mechanisms are in place to conduct the Offensive IO tasks that the division has the capability to execute.

As a final inquiry, the monograph analyzes the IO staff responsibilities outlined in the draft FM 100-6. The monograph identifies two tasks, establish and publish Offensive IO priorities, and battletrack Offensive IO, that were not assigned IO tasks. The monograph concludes that to conduct these tasks the division does not need a separate six soldier IO Coordination Cell, but rather one officer functioning much like the current FSCOORD or SOCOORD.

SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

Major Rosemary M. Carter

Title of Monograph: ***The Information Operations Coordination Cell - Necessary for Division Offensive Actions?***

Approved by:

_____ Monograph Director
COL Michael L. Findlay, MA

_____ Director, School of Advanced
LTC(P) Robin P. Swan, MMAS Military Studies

_____ Director, Graduate Degree
Philip J. Brookes, Ph.D. Program

Accepted this 7th Day of December 1998

TABLE OF CONTENTS

LIST OF FIGURES AND TABLES

Introduction

Dramatic changes in the missions of the U.S. Army and increased importance of the cybernetic domain of war have produced a review of current doctrine that is manifesting itself into one of the largest changes in Army doctrine this century. The change starts at the top with the soon to be published revision of FM 100-5, Operations, and is affecting all subordinate doctrine. This includes a major update to the Information Operations (IO) manual. Currently in its Integrated Concept Draft, the new FM 100-6 (re-titled Information Operations: Tactics, Techniques and Procedures, from its previous title of Information Operations) provides the fundamentals for planning and executing IO in the Army. The revised field manual (referred to as FM 100-6D throughout this monograph) is the doctrinal justification for an IO section within an Army Division with the primary mission to plan, synchronize, coordinate and deconflict Offensive IO and Defensive IO to support the commander.

Because of the increased use of technology to refine intelligence, facilitate decision making, enhance command and control, and improve lethality, Information Operations is growing in significance within the Army. Its importance has been recently validated for stability and support operations by US missions in Haiti and Bosnia Hercegovia. The need for a strong IO team for this type of operation is clear. However, the need for the IO cell in the other military actions is neither well defined nor validated. The current draft of FM 100-5 breaks military actions into four military actions: offense, defense, stability and support. This monograph questions the need for an IO coordination cell to conduct IO missions in a heavy division during offensive actions.

According to General Shalikashvili, then Chairman of the Joint Chiefs of Staff, in

the latest *National Military Strategy*, "the fundamental purpose of the Armed Forces must remain to fight and win our Nation's wars whenever and wherever called upon." This is in accordance with Title 10 the US Code, which mandates an Army that "shall be organized, trained, and equipped primarily for prompt and sustained combat."[1] With combat as the primary mission of the army, this monograph considers the role of IO and the IO planning staff during offensive actions. The research question is: Does the division need the Information Operations Coordination cell proposed in FM 100-6D to conduct IO during offensive operations? The answer is significant because of the valuable manpower resources dedicated to the new IO cell and the revisions to current division staff operations that must be implemented to fully integrate the IO cell into that staff.

Define Supporting Research Questions

This monograph answers the primary research question by answering three supporting questions. The first question lays the groundwork for the monograph: What IO tasks does the division need to execute in order to conduct offensive actions? The tool selected for determining these tasks is the Observe-Orient-Decide-Act (OODA) loop that was developed by COL John Boyd, USAF, to analyze a commander's decision cycle. COL Boyd's theory is an ideal tool to analyze the IO tasks because his theory is based on "isolating his adversary - physically, mentally, and morally - from is external environment by destroying his view of the world."[2] This theory is a stepping stone to IO as defined today.

The second research question is: What organic and habitual support capabilities does a heavy division have to execute the identified IO tasks? The organic capabilities

are determined based on the current Army TOE for an armor division. The habitual support capabilities are based on current doctrine for systems and capabilities that are provided to the division from outside organizations. An example of this is the Psychological Operations (PSYOP) cell that deploys with the division. The habitual support elements are from both Corps and EAC assets. Answering the first two questions provides a list of those IO tasks that are both relevant to the offensive fight and within the capabilities of the division.

The final research question is: What new staff mechanisms does the heavy division need to conduct these IO tasks using their identified capabilities? The monograph defines "conduct" in accordance with FM 101-5, Staff Organization and Operations. It is the planning, facilitating, and monitoring of functions. New staff mechanisms are needed for those IO tasks that are not currently conducted by the division staff.

The monograph conclusions and recommendations are based on the need for an IO staff section to execute the developed list of staff mechanisms. The monograph determines the requirement for the IO section based on three factors. First, it analyzes the responsibilities of the staff sections currently responsible for the Offensive IO tasks determined by the first research question using the capabilities determined in the second question. Any staff mechanisms that are not adequately performed by the current staffs are identified. Second, it considers the responsibilities of the IO section as outlined in FM 100-6D. These responsibilities are compared to the responsibilities of the current staff sections conducting Offensive IO tasks. Although this analysis is somewhat subjective, it is based on the doctrinal task responsibilities outlined in FM 101-5, Staff

Organizations and Operations. Finally, this section analyzes the job descriptions of the IO Coordination Cell from FM 100-6D to determine if the staff sections currently conducting the Offensive IO tasks are already performing these tasks. Any tasks not currently being performed are subjectively analyzed to determine if they require all or part of the proposed IO Coordination Cell to conduct them.

The final chapter sums up the finding of the monograph. It also proposes some alternative recommendations for executing IO in a division.

Establish Delimiters

The prominent delimiter to the monograph is the allocated length. It effects the entire scope of the monograph. It first limits the monograph to the IO portion of Information Superiority (see definitions). IO is defined as both Offensive IO and Defensive IO. Both forms of IO are used during all military actions. The limitation of this monograph to the Offensive IO piece does not negate the need for Defensive IO during all military actions. The limit is placed solely based on the length limitation. The analysis completed here for the Offensive IO tasks could easily be extended to the Defensive tasks.

The second significant delimiter is the analysis using only the offensive military action. As defined in the draft FM 100-5, Operations, there are four actions: offense, defense, stability and support. This monograph limits itself to the offense. This selection is based on the factors discussed in the introduction. When faced with the requirement to select only one military action, the logical selection is that action which is the primary mission of our armed forces and the most decisive form of action. Selecting offensive military actions also correlates with the selection of Offensive IO. The main IO effort

during offensive military action is Offensive IO. This monograph does not attempt to negate the importance nor simultaneity of the other three military actions nor Defensive IO. A future analysis of the need for a permanent IO coordination cell for the other military actions an Defensive IO is also suggested.

The length limitation also constrains this monograph to considering only one type of military unit. A division size element was selected from the choices of military units because it is the smallest warfighting headquarters for the Army that includes an IO coordination cell in the FM 100-6D. It is the integration point for the new IO staff concept into the tactical Army. FM 71-100, Division Operations, lists five types of divisions: Armored and Mechanized, Light Infantry, Airborne, Air Assault and Medium. Analysis of the capabilities of all five types of units was outside of the length limitation. Once narrowed to one type of division, the type and source document for that division had to be selected. In keeping with a more generic approach, rather than selecting one specific unit within the Army, the source document for the division is based on the armor division Table of Equipment and Organization (TOE).[3]

Another delimiter is the type of mission tasked to the division. This monograph considers only a division performing a conventional mission with a Corps as its higher headquarters. The missions and requirements for IO in a division serving as a Joint Task Force headquarters or Land Component headquarters are not considered. Once again, JTF and Land Component IO missions are important, but they are outside of the scope of this monograph.

The monograph also limits the division's capabilities. With ever changing requirements and capacities surrounding the Army Warfighter Experiments and the Army

After Next visions, the length of this monograph does not allow for analysis of all potential capabilities. In order to keep the monograph relevant to today's Army, it is limited to the equipment, systems and technology currently fielded in the US Army. However, the methodology used in this monograph remains relevant as new systems are fielded. The final delimiter is limiting the monograph to conventional operations. IO does include actions performed by special operations or other nonconventional forces.

The monograph is structured into six chapters. Chapter one, this chapter, is the introduction. It includes an introduction to the topic, defining the research questions, establishing the delimiters. Chapter two, Definitions, defines the doctrinal terms for Information Operations and military actions. It also introduces the FM 100-6 staffing of the IO section. Chapter three, Determining Necessary IO Tasks, uses the Boyd OODA loop to analyze Offensive IO tasks and determine which tasks affect the enemy commander's OODA loop. Chapter four, Determine Germane Capabilities, uses the armor division TOE to determine organic and habitual support IO capabilities. Chapter five, Assessment of Staff Mechanisms, determines if the division needs news staff mechanisms to conduct the necessary IO tasks. Chapter six is the conclusion and recommendations chapter.

Definitions

This chapter provides the baseline information for the monograph. The first section defines the Information Operations Terminology. The second section defines military actions in accordance with the final revised draft of FM 100-5, Operations dated 19 June 1998. The final section introduces the division IO staff section in accordance with FM 100-6D.

Information Operations Terminology

The area of Information Operations is evolving. Part of this evolution is coming to grip with the numerous sets of terms that define the environment. In current doctrine, the Army definitions are not nested within the Joint manuals. Additionally, the terms as defined in the FM 100-6D are different from definitions in FM 100-6, Information Operations, dated 6 December 1995. In order to limit any confusion during the analysis of FM 100-6D, all IO terms are defined here in accordance with that manual. Because the IO terms are confined to Army definitions, whenever possible this monograph will use the army definitions for other terms. However, when the army definition is nested within the joint definition, the reference for that definition defers to the higher level and thus the joint publications.

IO is defined in FM 100-6D as a subcomponent of the overarching practice of Information Superiority. Information Superiority (IS) is "that degree of dominance in the information domain which permits the conduct of operations without effective opposition. Army operations address it as a window of opportunity created by focused effort that allows the actions or beliefs of the enemy commander to be influenced in support of decisive operations."[4] IS is comprised of three interrelated components:

Relevant Information and Intelligence (RII),[5] Information Systems (INFOSYS)[6] and Information Operations. RII, fully defined in the notes, is in broad terms similar to the current Commander's Critical Information. INFOSYS, also fully defined in the notes, encompasses the physical systems that process information. Information Operations (IO) is defined as "offensive and defensive actions at each echelon in peace and war to defeat the adversary's command, control, computers, communications, intelligence, surveillance, and reconnaissance (C4ISR); affect adversary and influence neutral leaders; and protect friendly information and information systems plus the command and control process. The major IO capabilities are Operational Security (OPSEC), Psychological Operations (PSYOP), military deception, electronic warfare, physical destruction, and computer network attack. Related IO activities include public affairs, civil affairs, and other interactions with news agencies.[7] Figure 2.1, Linkage Between the Components of Information Superiority, provides a visualization of the relationship between these terms.

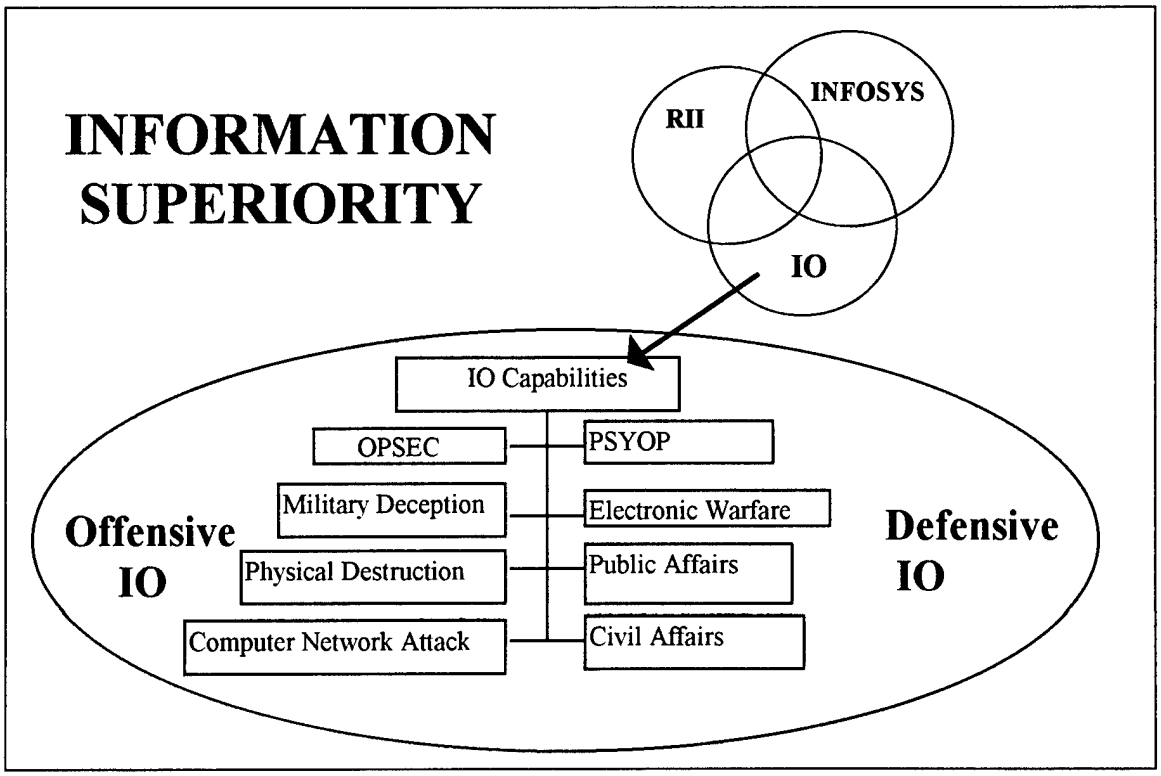


Figure 1.1 , Linkage Between the Components of Information Superiority

The delineation between offensive and defensive IO is relevant because this monograph limits itself to offensive IO. Offensive IO is defined as "the integrated use of assigned and supporting capabilities and activities mutually supported by intelligence, to affect adversary decision makers to achieve or promote specific objectives."[8] The IO capabilities that support Offensive IO include OPSEC, military deception, PSYOP, electronic warfare, physical destruction, special IO,[9] civil affairs, public affairs, and could include computer network attack." Defensive IO, fully defined in the notes, is steps taken to "protect and defend friendly information and information systems."[10]

The following are detailed definitions and descriptions of the Offensive IO capabilities as they relate to a division:

OPSEC. OPSEC is defined in FM 101-5-1, Operational Terms and Graphics, as all measures taken to maintain security and achieve tactical surprise. It includes countersurveillance, physical security, signal security, and information security. It also involves the identification and elimination or control of indicators, which can be exploited by hostile intelligence organizations. It is the protection of friendly information against enemy collection and exploitation. Although OPSEC is by nature a defensive action, it is considered Offensive IO when it includes actions taken to deceive the enemy in order to protect friendly information or action taken to conceal critical information. OPSEC is an integral aspect of any military operation but is critical during military deception operations. OPSEC is considered and planned for by all members of the division staff.

Military Deception. Military Deception is defined in JCS Publication 1-02, DOD Dictionary of Military and Associated Terms as "those measures designed to mislead the

enemy by manipulation, distortion or falsification of evidence to induce him to react in a manner prejudicial to his interests."[11] It further defines five categories: strategic military deception, operational military deception, tactical military deception, service military deception, and military deception that support OPSEC. For commanders at echelons corps and below, the primary categories of application are tactical deception and deception in support of OPSEC. These two forms of deception are combined in army doctrine and defined as battlefield deception - "those operations or measures conducted at echelons Theater and below to purposely mislead enemy forces by distorting, concealing, or falsifying indicators of friendly intent."[12] This level of deception relates to situations confronting tactical commanders. These plans are normally nested in the operational or strategic deception plans. Tactical commanders are not doctrinally precluded from developing independent deception plans, however, the complex planning process and need for completely synchronized deception plans at all levels of war normally prohibit independent plans.[13] Deception plans are coordinated by all staff sections that have staff responsibility for a portion of that plan. For example, the division signal office is responsible for planning the execution of a false electronic signature portrayed by a signal node. However, the division G3 has overall staff responsibility for division deception plans.[14]

PSYOP. According to Joint Publication 1-02, and FM 33-1, Psychological Operations, PSYOP are operations planned to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign government, organizations, groups and individuals. The purpose of PSYOP is to induce or reinforce foreign attitudes and behavior favorable

to the originator's objectives. The army's PSYOP assets are assigned to the US Army Civil Affairs and PSYOP Command (USACAPOC), a major subordinate command of the US Army Special Operations Command (USASOC). PSYOP support to the division comes from PSYOP Tactical Support Battalions, which reside in both active and reserve component forces. The battalion deploys a Division PSYOP Support Element (DPSE) to provide the commander with a tactical dissemination capability. Because the approval authority for PSYOP products is normally retained at theater level, the DPSE develops products for the division when requested, but must forward them to the approving authority level for further development and final approval.

Although the DPSE is not doctrinally required for a division to deploy, they are a habitual support element for divisions. This DPSE headquarters becomes part of the division G3 section. During offensive operations, the DPSE provides close, continuous support to the division with a focus on the exploitation of military actions to undermine the enemy's morale and will to fight. It may also support OPSEC or military deception operations.

Electronic Warfare. Electronic warfare is defined in FM 34-10, Division Intelligence and Electronic Warfare Operations, as "the use of electromagnetic or directed energy to degrade, neutralize, or destroy enemy combat capability."[15] It includes jamming and electromagnetic deception. EW consists of three areas: electronic attack (EA), electronic warfare support (ES) and electronic protection (EP)[16]. EA and ES are considered offensive EW. EA uses lethal (directed enemy) and nonlethal (jamming) electromagnetic energy to attack the enemy. EA also includes electronic deception. ES are actions taken to search for, intercept, locate and identify sources of radiated

electromagnetic energy. ES produces combat information. ES and EA as part of EW are considered elements of combat power just like fire and maneuver. When coordinated with the other forms of maneuver, EW can be an important part of the massing of effects on an enemy. EW is the staff responsibility of the division electronic warfare officer who works in the division G3 section.

Physical Destruction. Physical destruction is a normal part of any military operations. However, physical destruction that is aimed at destroying a target in support of the IO plan becomes a type of Offensive IO. An example is the destruction of critical command and control nodes prior to a major offensive action to disrupt the enemy commander's ability to see the battlefield. Physical destruction is the staff responsibility of the G3 section.

Civil Affairs. According to FM 101-5-1 and FM 41-10, Civil Affairs Operations, civil affairs (CA) are matters concerning the relationship between military forces deployed into a country or area and the civil authorities and people of that country or area. The CA mission is to support the commander's relationship with civil authorities and civilian populace, promote mission legitimacy, and enhance military effectiveness.[17] During operations, the division normally has a CA battalion attached. Under the staff supervision of the division G5, the CA Bn provides and facilitates civil-military actions between the division and the local populace or foreign military forces. Its missions include: minimize populace interference with military operations; advise the commander to meet moral and legal obligations; develop and implement the civil-military operations (CMO) plan; act as the focal point for cultural considerations that impact on military operations; and identify and coordinate requirements for host nation resources, facilities

and support.[18]

Public Affairs. Public Affairs (PA) is defined in JP 1-02 and FM 46-1, Public Affairs Operations, as those "public information and community relations activities directed toward the general public by the various elements of the Department of Defense. PA is necessary at the strategic, operational, and tactical levels of war to influence soldier morale, unit cohesion, (and) public opinion; affect strategic goals; impact operational objectives and have a bearing on tactical execution."[19] At the tactical level, PA must achieve a careful balance between OPSEC and flow of timely information. The division has a PA section that serves as special staff to the commander to provide him guidance on these issues. The section has operational control over all PA organizations assigned or attached to the division. When deployed, this PA section is augmented by a Mobile PA Detachment (MPAD). The MPAD includes a commander that augments the division PA staff and up to three teams that deploy in direct support to the combat brigades. Their missions, in coordination with the permanent division PA section, are to provide services and facilities for the civilian media representatives, process and distribute media products for the division, develop information strategies and campaigns in support of the operation, and support both higher and lower headquarters' PA requirements.

Computer Network Attack (CNA). CNA is a new term used in FM 100-6D to define actions taken to disrupt and destroy enemy computer networks. Defined as "hacker warfare" by Martin C. Libicki, of the Institute for National Strategic Studies,[20] it is the systematic attack of an adversary's computer systems. In scenarios played out at the highest level of military simulations, CNA is part of the attack plan.[21] However, the resources, technical skills and time required to plan and execute CNA make it extremely

difficult to perform at the tactical level. There are no division resources dedicated to planning, coordinating or implementing computer network attack.

Table 2.1 provides an overview of the Offensive IO capabilities and the division staff section that is doctrinally responsible for the capability.

Offensive IO	**Division Staff Responsibility**
Military Deception	G3 with support from required staff sections
Psychological Operations (PSYOP)	DPSE within the G3
Electronic Warfare (EW)	EW officer within the G3
Physical Destruction	G3
Civil Affairs (CA)	G5
Public Affairs	Special Staff
Computer Network Attack (CNA)	N/A

Table 2.1 Offensive IO Capabilities and Staff Responsibilities.

Military Actions Terminology

According to the Revised Final Draft of FM 100-5, Operations, dated 19 June 1998, there are four types of military actions: offense, defense, stability, and support. The four actions are inherent in any military operation. Operations are labeled as one type of action by the overarching action. However even operations that are considered predominantly one action retain some properties and characteristics of the other actions. An example is the campaign to liberate Kuwait in 1990/91. Operation Desert Storm was a defensive action designed to deter Iraqi aggression until the build-up of coalition forces

was completed. Operation Desert Storm was an offensive action designed to liberate Kuwait and destroy the Iraqi army. Operation Provide Comfort was a support operation designed to eliminate human suffering. All three operations are easily categorized but contain elements of the others. For example, during Desert Storm the coalition attack was supported by a continuing defense of key facilities in Saudi Arabia.[22] The final draft of FM 100-40, Tactics, dated 3 October 1998, (FM 100-4D) describes the interrelationships between these military actions as the Operational Continuum.[23]

The most decisive form of military action is the offense. It is defined in FM 101-5-1 as the principle of war by which a military force achieves decisive results by action with initiative, employing fire and movement, and sustaining freedom of maneuver and action while causing the enemy to be reactive.[24] Offensive operations are force oriented, terrain oriented or a combination of both. In FM 100-40D they are characterized by five sequential steps: gain and maintain enemy contact; disrupt the enemy; fix the enemy; maneuver; and follow through to exploit success and prepare for the next action. The purpose of the offensive is to: destroy enemy forces; seize terrain or facilities, denying them to the enemy; disrupt enemy attacks; deny the enemy resources; deceive and divert the enemy; fix enemy forces; and gain information.[25] Offensive actions allow our military forces to succeed in their foremost responsibility and prime consideration, (as outlined in the *National Military Strategy*, dated 1995) fighting and winning our Nation's wars. The other three military actions are defense, stability and support. They are fully defined in the endnotes. [26]

Information Operations Staffing

SECTION PERSONNEL	MISSION(s)
IO Coordinator (IOCOORD), LTC, FA 30	Overall responsible, coordinates directly with the commander, information manager for the division
IO Plans Officer, MAJ, FA 30	Integrates IO planning into the division plan, works in the division G3 plans cell, planning link to the IOCOORD
IO Targeting Officer, MAJ, FA 30	Integrates and coordinates IO targeting with division targeting, direct link to the ACE
IO Current Opns Officer, CPT, FA 30	Coordinates and monitors execution of IO from DIV TAC, the link between the IOCOORD and the current fight
IO NCO, SFC, 11M50	Coordinates activities of the IO section; produces IO products, provides 24 hour IO synchronization
Info Systems Opns Analyst, SFC, 74B50	Direct link to the Div Signal Office (G6) for defensive IO. Provides interface with G6 for automation support.

Table 2.2, Division IO Section with Individual Missions/Responsibilities.

FM 100-6D establishes the division IO section that has staff responsibility for IO actions within the division. A special staff section that reports directly to the division chief of staff, the section has numerous responsibilities that include: establishing IO priorities for the division; synchronizing, coordinating, and deconflicting Offensive and Defensive IO to support the commander's intent; recommending taskings to the G3 for the assets necessary to execute IO; coordinating IO input into the paragraph three of the division orders and writing the IO annex; coordinating intelligence support for IO; and coordinating with higher and lower headquarters for IO issues. Table 2.1, Division IO Section with Individual Missions/ Responsibilities, provides a graphic depiction of the section. The titles, ranks, and missions are from Chapter two of FM 100-6D.

IO Tasks

FM 100-6D defines information superiority as the window of opportunity that allows the friendly commander to influence the actions or beliefs of the enemy commander. IS is a result of actions degrading the enemy's decision cycle while protecting and enhancing the friendly decision cycle. This chapter analyzes the actions of Offensive IO on the enemy's decision cycle by determining which IO tasks have the potential to disrupt or interrupt the cycle.

The concept of beating the enemy by out-thinking him dates back to the beginning of warfare. Sun Tzu in his much studied The Art of War articulated that in order to defeat the enemy "you must keep your opponent dancing to your tunes. It is important that you are always the initiator, and your opponent the one who reacts."[27] Sun Tzu also dedicated an entire chapter to the necessity for and benefits of secret spies that provide the commander with the ultimate foreknowledge about the enemy's actions and reactions. Frederick the Great concurred with this in his writings that were published in 1747 as The Instruction of Frederick the Great for his Generals. He stated that "it is essential to know what is happening among the enemy."[28]

Napoleon Bonaparte also was concerned with beating the enemy's decision cycle. In his maxims first compiled by General Burnod and published in 1827, Napoleon was quoted as saying that "the first principle of a general-in-chief is to calculate what he must do, to see if he has all the means to surmount the obstacles with which the enemy can oppose him and when he has made his decision, to do everything to overcome them."[29] He understood that a great general must be able to get inside the enemy's head, determine his courses of action, and have plans to defeat all of those possible courses of action.

The maxim was carried into modern theory by numerous writers to include Major General J.F.C. Fuller, British Army. Fuller said "the physical strength of an army lies in its organization, controlled by its brain. Paralyze this brain and the body ceases to operate."[30] The US military adapted this theory into its doctrine. The current FM 100-5, Operations, dated June 1993, Chapter two, Fundamentals of Army Operations, states that the role of the Combined Arms team is to "confuse, demoralize, and destroy the enemy with the coordinated impact of combat power. The enemy cannot comprehend what is happening; the enemy commander cannot communicate his intent nor can he coordinate his actions. The sudden and devastating impact of combined arms paralyzes the enemy's response, leaving him ripe for defeat."[31] This is incorporated in the draft FM 100-5, dated 19 June 1998, in Chapter Six, Execution. It states that "Army forces detect, monitor, exploit and, when authorized, attack enemy information and information systems and manipulate the enemy's operational picture. In attacking enemy information and systems, the commander focuses on the effects and not solely on the targets. Under attack, the enemy's situational awareness deteriorates. The enemy commander's decision cycle slows."[32]

The OODA Loop

One of the more recent writers on the decision cycle was Colonel John Boyd, US Air Force. COL Boyd gained a reputation in both the air force and throughout the Department of Defense, first as an F-86 pilot in the Korean War, and then as an engineer assisting the Air Force in the aeronautical design of fighter aircraft. COL Boyd became the first theorist to combine aspects of logic theories with the laws of thermodynamics when he completed his "Destruction and Creation" study on the relationships between

competition and conflict. Originally, a highly abstract consideration of the friction between order and disorder, COL Boyd combined this theory with a thorough study of military theorists and great leaders to develop the OODA loop hypothesis. Boyd's OODA loop views any conflict as a battle where

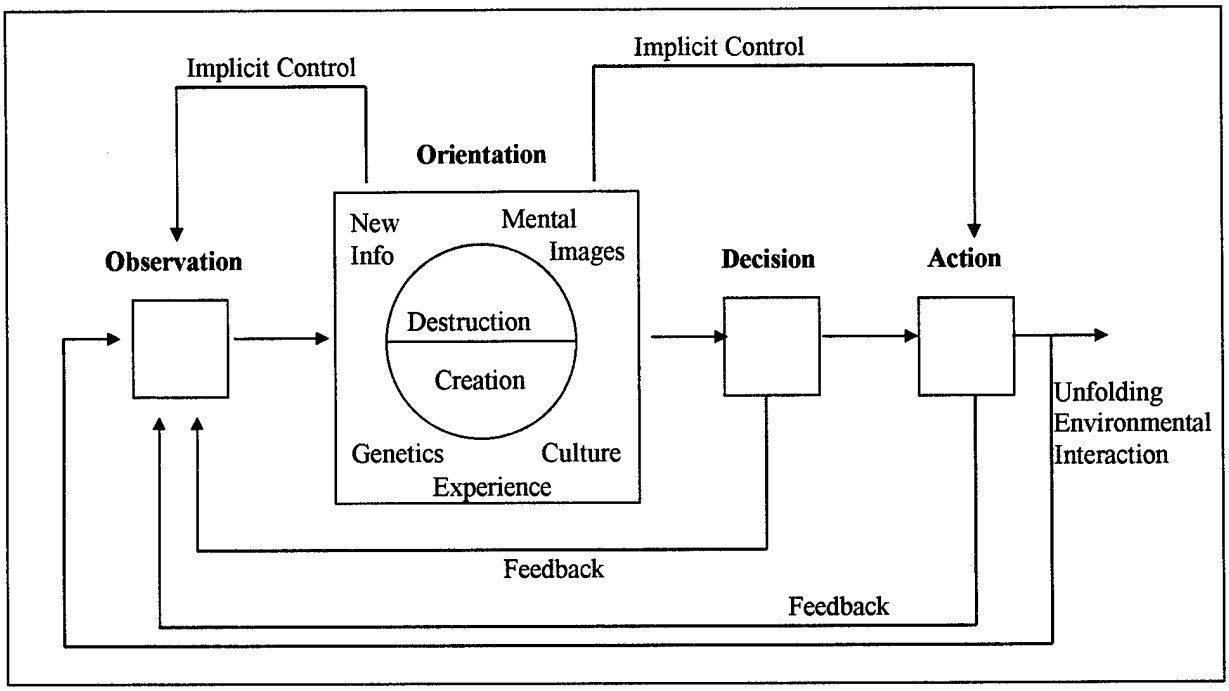


Figure 3.1 Boyd's OODA Loop

each leader must observe (O) his enemy, orient (O) himself and his forces to best challenge the enemy, decide (D) on the most appropriate action, and act (A).[33] The hypothesis is describes as a loop because it is a continuing cycle with feedback at every level. Figure one is a visual depiction of the OODA loop from MAJ David Fadok's thesis on the subject.[34] COL Boyd argued that the U.S. military's tactics, strategy, and technologies should all be based on executing our OODA loops faster than the enemy -- getting inside of his decision cycle by executing our faster.

Using the stages of Boyd's OODA loop - observe, orient, decide and act - as the

criteria, the following analysis determines which Offensive IO capabilities are necessary to achieve IS during offensive operations. The capabilities are measured based on their ability to degrade the enemy commander's OODA loop. The ultimate goal is stop the enemy commander's OODA loop process entirely by creating chaos within his organization.

Military Deception

Military deception influences the enemy commander's ability to observe the battlefield. Its goal is to induce the opposing commander to make decisions that support the friendly commander's intent. Military deception can also entice the enemy to orient his forces, collection assets and combat power in the wrong direction (from his perspective) or with improper timing. By impacting on the observe and/or orient stages, deception affects the decision step. Here is where the success of military deception is evaluated. A successful plan forces the enemy commander, defined as the target of the deception, to make a decision that is exploited by the friendly plan. Whatever action the enemy takes becomes the choice of the friendly commander as defined in the objective of the military deception. When properly executed, military deception affects all four stages of the enemy commander's OODA loop.

PSYOP

PSYOP can also impact the enemy commander's entire OODA loop by affecting his accuracy in observation and orientation. As an enhancement tool for a military deception plan, PSYOP can use audiovisuals, printed materials, and media broadcast to support the deception plan. By supporting the overall offensive mission, PSYOP serves as a combat multiplier, setting conditions or supporting military actions to achieve

decisive results. In this role, PSYOP can affect the enemy commander's ability to observe. An overwhelming PSYOP campaign can also impact on the enemy commander's personal psyche extending the time required for him to make decisions even in the presence of seemingly accurate information.

EW

According to FM 34-10, Division Intelligence and Electronic Warfare Operations, EW supports four functional elements of Command and Control Warfare (C2W): destroy, deceive, disrupt and defend. Three of these functions, destroy, deceive, and disrupt, are applicable to the offense. Destruction is the actual removal of the enemy's command, control, communications, computers and intelligence (C4I) ability. EW supports destruction through lethal EA using newly developed and developing directed energy weapons. EW supports disruption through jamming. Jamming degrades the enemy's communications capability, which can affect the entire OODA loop. Poor or severed communications can slow observation reporting; slow the orientation of collection and other assets, leave the commander with limited intelligence for making decisions, and degrade transmission of orders on the battlefield. Jamming that affects one of these actions slows the OODA loop. Jamming that can affect all four steps may drastically limit the enemy commander's ability to have any influence on the battlefield. One key limitation of jamming is timeliness. Once the enemy detects jamming, he will begin countermeasures. Therefore it is key to execute jamming at the most decisive point to gain the desired effects.

EW deception is conducted through simulative electronic deception (SED), manipulative electronic deception (MED) and imitative electronic deception (IED).

These electronic deception measures, whether in support of a larger military deception plan or a stand-alone activity, affect the enemy commander's OODA loop in the same fashion as any successful military deception.

During movements to contact, the primary purpose of EW is to identify, locate and collect technical data on key enemy emitters.[35] Jamming is normally minimal to limit the enemy's ability to detect friendly forces and intent. Intercept priorities are normally C2 nets (maneuver, fire support, engineering), intelligence nets and jammers. During the attack, the EW priorities remain the same; however, they selectively jam key enemy C2 nets during critical points in the attack to disrupt the enemy's decision cycle. EA lethal systems are integrated into the overall plan of the attack. EW assets are normally concentrated to support the main effort. Additionally, assets may be focused primarily on enemy fire support nets to limit the combat effectiveness of indirect fire systems. In each of these capacities, EW interferes with the enemy commander's ability to observe and orient his assets for making timely decisions.

Physical Destruction

In accordance with Chapter 4 of the draft FM 100-40, "offensive operations are combat operations designed primarily to destroy the enemy."[36] Destruction of the enemy's C4I system affects the enemy commander's entire OODA loop. The effects are similar to those discussed during EW jamming of C4I; however, the results are long term rather than the shorter, temporary nature of jamming. At the least, physical destruction of C4I will affect the OODA loop during the reengineering of communications networks, re-establishment of reporting procedures, and rebuilding of headquarters. The effects will be longer term if the C4I system was a one-of-a-kind system or not part of a

redundant system. An example is a key communications site linking tactical operations centers (TOCs) across difficult terrain. Destroying that site may have short term effects on the OODA loop if the traffic can be rerouted through the network. However, if that site is the only link between the TOCs, it may take the enemy much longer to reestablish communications with its subordinate unit(s).

CA

Civil affairs activities establish a relationship with the local populous. Although CA personnel are not intelligence providers,[37] they are in an excellent position to collect information and forward that information to intelligence personnel for analysis. This information can be used to influence the enemy commander's decision step. CA can also affect the steps more directly. CA operations can generate or reinforce local popular support for US forces. This can eliminate intelligence sources for the enemy commander, reduce his observe capability and slow his decision process.

PA

Public affairs support the offense because it "nurtures and sustains public confidence in the Army's ability to get the job done and take care of its people."[38] It also is an effective tool to keep US soldiers aware of the current situation. During the offense, the balance between open, honest access must be very carefully weighed against OPSEC requirements. While this can be an enormous task for the division's PA section, it is primarily a defensive mechanism. The PA section may plan and execute a public relations platform as part of an offensive operation, but it is not designed to target or effect the enemy commander. Information that targets the enemy is considered PSYOP. Therefore, the IO capability of PA is not designed nor executed to affect the enemy

commander's OODA loop.

CNA

As stated in Chapter two, computer network attack is beyond the scope of a tactical division. While it is feasible that the division IO section may request a computer network attack as part of an offensive operation, the time required to plan and execute such an attack makes it unrealistic in all but the most abstract hypothetical examples. CNA may affect a commander's OODA loop; however, it is not planned or executed at the division level.

This chapter considered each of the Offensive IO tasks and used the Boyd's OODA loop to determine which tasks affect the enemy commander's decision cycle. Military deception, psychological operations, electronic warfare, physical destruction, and civil affairs are all actions that can be used at division level to gain IS by degrading the enemy commander's decision cycle. Public affairs are not planned to directly impact on the enemy commander's OODA loop. Any effects are secondary and cannot be considered an attribute of public affairs operations. Computer network attack may affect an adversary's OODA loop, but is not planned or executed at the tactical division level.

Determine Germane Capabilities

The US army division is a tactical unit that fights and trains as a combat team. It is designed to be largely self-sustaining, capable of executing independent maneuver on the battlefield. According to FM 71-100, Division Operations, US armor divisions:

> "are employed to maximize mobility, survivability, lethality and psychological effects (shock) on the enemy. These divisions destroy enemy armored forces. They can seize and secure land areas and key terrain. During offensive operations, armored divisions can rapidly concentrate overwhelming lethal combat power to break or envelop enemy defenses or offensive formations. These divisions then continue the attack to destroy fire support, command and control, and logistics elements. Their mobility allows them to rapidly concentrate, attack, reinforce, or block enemy forces. Their collective protection systems enable them to operation in a nuclear, biological and chemical (NBC) environment. Armored divisions operate best in open terrain when they gain the advantage with their mobility and long-range, direct-fire weapons"[39]

The standard armored division is a 17,500 soldier unit equipped with numerous weapon systems to include: 317 M1A2 tanks, 238 Bradley Fighting Vehicles, 54 self propelled howitzers, 24 AH-64 Apache attack helicopters, and 16 OH-58D(I) Kiowa Warriors. It has the capacity to bring destroy symmetric enemy forces. In addition to its unprecedented combat power, the division can conduct Offensive IO assets. This chapter determines the organic and habitual support systems that the division has to perform the IO tasks that were determined to be relevant to offensive operations. Those IO tasks are military deception, PSYOP, EW, physical destruction, and CA.

Military Deception

At the division level, there are no dedicated resources for military deception. However, since most systems can be used in a deception role, the resources available for military deception are limited only by conflicting requirements which often must support the actual operation and the resourcefulness of the planner. Success of military deception

depends on a realistic depiction designed for the collection assets of the enemy. There are two categories of materials required for military deception - hiding-the-real and portraying-the-false.[40] Hiding-the-real resources are used to eliminate enemy detection of friendly operations. They include camouflage, smoke, engineer equipment and EW assets. Portraying-the-false resources are those systems used to present a deception. They are further divided into visual and electronic systems. Visual resources are those used to deceive the enemy's "eyes" that may include: high resolution satellites, UAVs, strategic and tactical air reconnaissance, and soldiers. Electronic systems are the electronic warfare systems and other communications systems used to portray real networks.

Division military deception assets are the same assets used for real operations. Therefore, the division must weigh the benefits of dedicating these resources to a military deception against other operational requirements. Additionally, a deception operation takes a tremendous planning effort that must be allocated away from other operations. The division has only one planner designated as a division deception planner (who certainly has additional responsibilities in the division G3 section). All other planners come from the general planning staff.

Because of the planning and resource constraints at the division level, most deception operations are planned at higher echelons. The division supports these plans with resources and the detailed planning needed at the division level to execute the mission. However, if the division commander decides to execute an independent division deception plan, it must be synchronized and nested with the overall corps plan and any other deception plans. It is a major event for the entire division planning staff.

PSYOP

The only organic PSYOP asset in the division is the G3 PSYOP cell consisting of a 39B PSYOP Major and 37F40 Psychological Operations NCO. Their cell is habitually augmented during deployments by a division PSYOP support element (DPSE) from the attached tactical PSYOP company of the PSYOP Tactical Support Bn. The DPSE consists of approximately eight soldiers that form the division's staff planning section for psychological operations. The DPSE has limited PSYOP product development capability for products for the immediate use in the division's area of operations (AO). The approval authority for PSYOP materials rarely rests with the division commander, so higher headquarters approval is necessary. The DPSE normally deploys with one MSG-85B audiovisual system. It has a 350 watt backpacked loudspeaker, a multiband receiver, a mobile editor/dubbing station, a wide screen video projection unit, a video camera, 35-mm still camera, a Polaroid camera and a Canon paper copier.[41] The DPSE coordinates the actions of the Brigade PSYOP Support Elements (BPSEs) located with the maneuver brigades. The BPSE serves as a staff section within the brigade, with no product development capabilities. Besides integrated staff operations, the BPSE also coordinates the actions of the Tactical PSYOP Teams (TPTs) normally attached OPCON to the maneuver battalions. The TPTs can disseminate PSYOP products, conduct face-to-face PSYOP in the battalion's area of operations (AO), conduct loudspeaker operations, and evaluate the effectiveness of PSYOP on the local population. The TPTs normally deploys with mounted and/or dismounted loudspeaker systems that have ranges from 100 to 1,800 meters depending on the model.

EW

The Division G3 is overall responsible for the planning, integrating and synchronizing of EW into division operations. The G2, Fire Support Coordinator (FSCOORD), and Assistant Division Signal Officer (ADSO) provide input to the G3 EW officer for the EW plan. The division's electronic warfare assets are in the division's aviation brigade and military intelligence battalion. In accordance with the current Table of Equipment and Organization (TOE) for a heavy division[42] and FM 34-10-2, Intelligence and Electronic Warfare Equipment Handbook, the EW assets include: the AN/TLQ-17A(V)3 TRAFFICJAM a VHF EA system designed for surveillance and jamming; the AN/TRQ-32(V)2 TEAMMATE that intercepts HF, VHF, and UHF communications signals to provide direction finding and recording of enemy traffic; the AN/TSQ-138 TRAILBLAZER that is a HF, VHF, and UHF intercept system and a VHF direction finding support system. These three systems are scheduled to be replaced by

SYSTEM	CAPABILITIES
AN/TLQ-17A(V)2 TRAFFICJAM	VHF EA
AN/TRQ-32(V)w TEAMMATE	HF, VHF, and UHF ES
AN/TSQ-138 TRAILBLAZER	HF, VHF and UHF ES
IEW Ground Based Common Sensor (GBCS)	HF, VHF and UHF ES/EA
AN/PPS-5B Radar Set	portable, battery operated ES
AN/ALQ-151(V)2 Quickfix (EH-60A)	VHF ES/EA
Unmanned Aerial Vehicle (UAV)	ES/EA

Table 4.1, EW Systems and their Capabilities

the IEW Ground Based Common Sensor (GBCS) that is currently being fielded with some delays.[43] The IEW GBCS is intended to eliminate the current diverse systems at division, corps and EAC levels. It heavy configuration includes both ES and EA capabilities with interface to aerial platforms. The division also has AN/PPS-5B Radar Sets that are portable, battery operated systems used to locate, identify and track moving ground targets; the AN/ALQ-151(V)2 Quickfix IIB aircraft in the EH-60A configuration that can receive, locate and jam VHF communications; and Unmanned Aerial Vehicles that are designed to operate forward of the FLOT (forward line of troops) providing reconnaissance, surveillance, and are projected to provide ES/EA capabilities in the future. In addition to its own assets, the division requests EW support from Corps and Echelons Above Corps (EAC) assets (an example is the US Air Force COMPASS CALL platform) and has several automated systems for receiving feedback to include the TROJAN Special Purpose Integrated Remote Intelligence Terminal (SPIRIT), AN/TSQ-168(V) JSTARS terminal, and the All-Source Analysis System (ASAS). With its organic systems and the broad corps and EAC assets available, the division can execute a robust EW plan in support of the overall offense. The operation of the MI Bn's EW assets is planned by the division EW officer with extensive input from the Bn S3 and the G2's Analysis and Control Element (ACE). The division EW officer is overall responsible for planning the aerial EW platforms in conjunction with both the G2 and the division G3 air/aviation planners.

Physical Destruction

Physical destruction is the main planning effort of the entire division G3 section during offensive operations. The objective is "to close with and defeat the enemy while

minimizing risk to our soldiers."[44] Physical destruction that targets the enemy C4I structure is integrated into the overall plan. However, special emphasis is placed on destruction of enemy C4I in the deep fight. The deep operations coordination cell (DOCC) plans the deep fight "to destroy, delay, disrupt, or divert critical enemy elements not currently engaged in the close fight."[45] Deep operations target high payoff targets such as enemy C4I, artillery, air defense artillery, air forces, sustainment bases, and reserve maneuver forces. The division uses the targeting process to allocate resources for detecting targets, engaging targets and conducting battle damage assessments (BDA). All forms of lethal and nonlethal weapons are considered in the targeting process to include: EW, attack helicopters, indirect fires from either army or navy assets, army tactical missile systems (ATACMS), and air interdiction.[46] In some cases based on its proximity to the FLOT, C4I may be targeted by ground maneuver forces. Additionally, the division staff has avenues for requesting physical destruction support against C4I targets from a myriad of Corps and EAC assets to include corps artillery, corps aviation, naval gun fire and air force aviation. In any case, the priority of effort place on enemy C4I is weighed against the division's other priorities to develop an integrated and synchronized plan that supports the overall commander's intent and higher headquarters' tasks to the division.

CA

The division's organic CA capability is the G5 section. However, all divisional units conduct civil military operations to some extent. The G5 is authorized a 39C Civil Affairs Lieutenant Colonel, a 39C Civil Affairs Major and administrative support to coordinate, synchronize and provide expertise for these civil military operations. They

are habitually supported by a direct support (DS) CA battalion. The battalion is composed of a Direct Support Detachment that serves works closely with the division CA planning staff, and four Direct Support Teams (DSTs) that perform basic CA functions under the control of the subordinate units. These DSTs can deploy with the maneuver brigades or with other units, such as the DISCOM, that require CA support. The CA BN does not have specialized CA teams. Specialized teams are located in the general support (GS) CA Bn OPCON to the corps that provides CA services on an area basis. These teams include: dislocated civilian teams, public communications teams, public works teams, public health teams, public administration teams, civilian supply teams, civil defense teams and language teams. Specialized support is requested through the division G5 to the corps G5 or division higher headquarters.

This chapter considered the organic and habitual support systems that the heavy division has to perform the Offensive IO tasks of military deception, PSYOP, EW, physical destruction, and CA. The division with its organic combat, combat support and combat service support assets can conduct military deception, physical destruction and EW. Military deception requirements are resourced from within the division. Physical destruction mechanisms are located throughout the combat units of the division. The division has assets in its aviation brigade and military intelligence battalion for electronic warfare. However, the division only has organic planning staffs for PSYOP and CA. The division receives habitual support PSYOP support elements consisting of the DPSE, BPSEs and TPTs to execute tactical psychological operations. CA Bn (DS)'s habitually provide civil affairs teams to augment the division staff and some subordinate elements. A CA Bn (GS) provides specific civil affairs support as required.

All four areas of Offensive IO have capabilities at Corps and higher that are also available through coordination and requests. The division's staff sections are responsible for requesting, coordinating and synchronizing any support from outside organizations. The division staff's overall responsibility for Offensive IO is the focus of the chapter five.

Assessment of Staff Mechanisms

This chapter assesses the current staff mechanisms for conducting the Offensive IO tasks relevant to offensive operations. The tasks are military deception, PSYOP, EW, physical destruction and CA. The chapter identifies the primary staff agency responsible for the task and any supporting staff. It includes the staff agency's overall staff responsibilities and how they apply to the Offensive IO task. The question for each Offensive IO task is "What new staff mechanisms does the division need to conduct this task?" The chapter concludes with a subjective evaluation of the IO Coordination Cells proposed task list and determines if there are any unique tasks listed in FM 100-6D that require a new staff mechanism.

Doctrinal Staff Responsibilities

Military Deception. Military deception is the primary responsibility of the deception officer in the division G3 section. In accordance with FM 101-5, the deception officer is "the special staff officer for coordinating deception assets and operations for the command. The deception officer comes from the MI battalion, but is not normally the commander of the supported unit. Besides his common staff responsibilities, the deception officer's specific responsibilities are as follows:

- Exercises staff supervision over deception activities.
- Determines, with the G2, requirements or opportunities for deception operations.
- Recommends to the G3 the deception target, objectives and deception story.
- Integrates use of deception assets.
- Monitors execution of the deception plan."[47]

Military deception is a complicated process even in its simplest form because it

requires all of the detail of an actual operation with the added requirement of identifying the objectives, target, and story. For division level deception planning, the deception officer must weigh the importance of the deception against other missions and make a recommendation to the division G3 carefully considering the second and third order effects of the deception on division resources. Because a deception plan must be carefully nested in the higher headquarters' plan, the deception officer closely coordinates division deception plans with the corps deception officer. The deception officer also closely coordinates deception plans with the appropriate staff sections. For example, a deception plan that includes an electronic signature of a signal node must be coordinated with the Assistant Division Signal Officer (ADSO) for frequency assignments, and the implications of dedicating the signal battalion's assets. A deception plan that includes a build-up of logistics supplies at a port location must be coordinated with the G4 for shifting of assets to that port. It may also require dedicated transport assets, and a material management section from the DISCOM. The listing of deception officer responsibilities in FM 101-5 includes all of these tasks. There are not any new staff mechanisms required for military deception as a part of Offensive IO.

PSYOP. PSYOP planning and coordination is the responsibility of the division PSYOP officer who is authorized in the division G3 with a 37F40 PSYOP NCO.[48] In accordance with FM 101-5, "besides his common staff responsibilities, the PSYOP officer's specific responsibilities are as follows:

- Exercises staff planning and coordination over PSYOP activities.

- Evaluates, with the G2 and G5, enemy PSYOP efforts and the effectiveness of friendly PSYOP on target groups.

- Coordinates with the G5 for the impact of PSYOP.

- Coordinates audience pretesting and post testing for propaganda and counter-propaganda products.

- Coordinates with the G5 for the planning of and assistance with the execution of dislocated civilian operations.

- Evaluates the effectiveness of the PSYOP campaign on the target audience.

- Evaluates the psychological impact of military operations on the enemy and civilian populace.

- Coordinates with the PAO and G5 to ensure information messages being disseminated are consistent."[49]

During offensive operations, PSYOP is often considered "one of those other means available"[50] to support the division commander. In its supporting role, it must be carefully integrated into the operation. The PSYOP staff officer works closely with the division operation officers for this to be effective. The PSYOP staff officer also works closely with the division PSYOP support element (DPSE) to maximize their contribution to the operation both by executing PSYOP missions within their capabilities, and recommending employment options for the tactical PSYOP teams (TPTs) where they can be most effective in the division. The responsibilities listed in FM 101-5 and FM 33-1, Psychological Operations, include close coordination of PSYOP capabilities. There are not any new PSYOP staff mechanisms that must be performed to support Offensive IO.

EW. The division EW officer works for the division G3 planning, facilitating and monitoring electronic warfare activities. In accordance with FM 101-5, "besides his common staff responsibilities, the electronic warfare officer's specific responsibilities are

as follows:

- Assists in coordinating C2-attack and C2-protect concepts to support the commander's concept of the operations.

- Coordinates, prepares and maintains the electronic warfare target list, electronic attack taskings, and electronic attack requests.

- Coordinates with the G6 to deconflict frequencies and the joint restricted frequency list with EW targets.

- Coordinates with the Technical Control and Analysis Element (TCAE) to identify opportunities for effective targeting using jamming, deception, and PSYOP.

- Participates in the targeting meeting."[51]

The EW officer does not plan the use of EW assets in isolation. Electronic warfare assets must be considered in conjunction with other methods of targeting the enemy in order to mass effects and economize the use of force. The division targeting board and targeting meetings are the staff mechanism for synchronizing all fires (both lethal and nonlethal). The EW officer is a critical and active participant in the boards. EW assets are one of the largest arsenals that the division has to conduct Offensive IO, however, the EW officer working with the G2, G3, MI Bn staff, Avn Bn staff and FSCOORD has all of the staff mechanisms in place to execute EW. There are not any new EW staff mechanisms that must be performed in order to execute Offensive IO.

Physical Destruction. The division G3 is the principal staff officer for all matters concerning planning and operations. His list of responsibilities also includes the areas of training, force development and modernization. A detailed list of all of his responsibilities is found in FM 101-5, Staff Organization and Operations. A complete list

of his responsibilities for operations and planning is located in Appendix A of this monograph, G3 Staff Responsibilities for Operations and Planning. Responsibilities from FM 101-5 that are key to planning physical destruction are:

- Participating in targeting meeting.

- Synchronizing tactical operations with all staff sections.

- Monitoring the battle.

- Integrating fire support into all operations.

- Recommending priorities for allocating critical command resources.

- Recommending use of resources to accomplish both maneuver and support, including resources required for deception operations.

- Participating in course of action and decision support template (DST) development with the G2 and FSCOORD.

- Recommending task organization and assigning missions to subordinate units. The division G3 section is fully staffed to conduct the complex myriad of tasks necessary to execute physical destruction. The overall G3 section is divided into sections for training, operations, plans and exercises, and force development/modernization. In addition to the permanently assigned members of the section, the G3 also has coordinating staff responsibility for numerous special staff officers to include: air defense, air force air, naval air and gunfire, army aviation, chemical, engineering, explosive ordinance disposal (EOD), and fire support. In most cases the division's actual special staff officer for these functions is also a commander. An example is the fire support coordinator (FSCOORD) who is also the division artillery commander. These commanders designate an assistant that works either for or with the G3 for planning,

synchronizing and executing their specific staff tasks (i.e. the AFSCOORD).

As discussed in chapter four, the division may form a DOCC at the main command post to focus on the deep fight that targets enemy command and control. Based on mission, enemy, terrain, troop, time, and civilian considerations (METT-TC) the DOCC may work directly for the division commander or assistant division commander for maneuver (ADC(M)). However, the division G3 retains overall staff responsibility for the synchronization of all operations.[52] When the G3 and/or DOCC plans to engage enemy C2 with indirect methods, the division's targeting meeting is the primary forum for planning and synchronization. When the G3 plans to engage enemy C2 with maneuver forces, the division operations order includes tasks to subordinate units that are planned and synchronized in the military decision making process. The division does not require any additional staff mechanisms to conduct physical destruction for Offensive IO.

CA. In accordance with FM 101-5 the division G5 (Assistant Chief of Staff, Civil-Military Operations) is the principal staff officer for all matters concerning civil-military operations. The G5 has the responsibility to enhance the relationship between military forces and civilian authorities and personnel in the area of operations. Appendix B, G5 Staff Responsibilities, has the complete list of CA staff responsibilities in accordance with FM 101-5, Staff Organizations and Operations. The twenty-five listed tasks provide a detailed synopsis of civil affairs responsibilities for all four types of military actions. The specific tasks that apply to the offense are based on METT-TC, however the overarching responsibility is to minimize civilian interference with the combat operations. To accomplish this, the G5 must develop a detailed intelligence

estimate on the civilian population in the division's AO. This requires close coordination with the division's G2 section. The G5 uses that estimate to develop an integrated plan for minimizing civilian interference. The plan must be nesting in the division's overall plan so it must be closely coordinated with the G3 and other staff sections. The complete list of staff responsibilities includes the staff mechanisms to execute all of these CA tasks. The division does not require any additional mechanisms to conduct CA in Offensive IO.

Analysis

The staff mechanisms necessary for independently conducting the five Offensive IO tasks (military deception, PSYOP, EW, physical destruction, and CA) are already in place. Both FM 101-5, Staff Organization and Operations, and the specific field manuals for the five tasks provide detailed and clear delineation of responsibilities for these tasks. What is not yet resolved, is the need for the IO Coordination Cell to synchronize the five tasks under the overarching objective of Offensive IO. The resulting question is "Does the division need additional staff mechanisms to integrate and synchronize the individual IO tasks?" This question is answered by determining if the staff sections responsible for the Offensive IO tasks are currently integrated and synchronized.

EW and PSYOP assets are often used as part of military deception plans so their staff sections must be included in the planning. According to FM 33-1, Psychological Operations, "PSYOP can markedly enhance deception operations. .... PSYOP personnel and equipment have inherent capabilities and requisite skill that make them ideally suited to support the planning and execution of deception operations."[53] Besides the material items that the PSYOP teams can provide for deception plans, PSYOP trained soldiers are

also excellent at determining the enemy target's reaction to a given scenario. This makes them extremely valuable to the deception planner. Because of the close relationship between EW and military deception, electronic attack (EA) contains a category of electromagnetic deception. Electromagnetic deception, which "causes the enemy to misinterpret what is received by his electronic systems."[54] This deception may be used as an independent action or in conjunction with a more complex deception plan based on the enemy's collection capabilities and the division's deception objectives. In either case, the EW officer works closely with the deception officer to develop, and monitor the plan.

Similar to the relationship between the deception, PSYOP and EW officers is the relationship between the PSYOP officer and the G5. According to FM 71-100, Division Operations, "although (PA), CA and PSYOP each have some discreet audiences with tailored messages, the information overlap between their audiences is growing. The different messages must not contradict one another or the credibility of all three is lost."[55] The widespread and real-time influence of the world's media greatly influences this connection because messages normally can no longer be targeted at only one of the audiences. Ideally, the three staff sections will develop their information campaigns in concert, but even if they plan in isolation, they must synchronize the end results to maintain credibility.

Finally, all four of the other staff sections (deception, EW, PSYOP, and G5) are mandated by FM 101-5 to coordinate their planning and operations with the division G3. Three of them - the deception officer, EW officer, and PSYOP officer - actually work in the division G3 section. The G5, although a separate staff section, is directed in FM 101-5 to perform seven tasks that require direct coordination with the G3 section. They are:

"minimizing civilian interference with combat operations, to include dislocated civilian operations, curfews, and movement restrictions; advising the commander on the employment of other military units that can perform CMO missions; coordinating with the G3 (FSCOORD) on protected targets; coordinating with the G3 (PSYOP) on trends in public opinion; coordinating with the PAO and G3 (PSYOP) to ensure disseminated information is not contradictory; coordinating with the G3 (PM) the planning of the control of civilian traffic in the area of operations; and assisting the G3 with information operations."[56] Several others, found in Appendix B, imply coordination with the G3 section. Whether through direct contact due to working relationships, or the staff responsibilities outlined in FM 101-5, the four staff sections who have staff responsibility for deception, EW, PSYOP, and G5 work closely with the division G3 section. Because this G3 section is responsible for physical destruction, the mechanisms are in place for any required coordination. Also, the division's targeting meeting provides a structured format for synchronizing the Offensive IO tasks. This analysis shows that the staff mechanisms are currently in place to integrate and synchronize the division. The 'synchronize IO' task is already being executed by the involved staff sections. Therefore, the division does not need an IO Plans Officer who primary function is to execute this task.

The division does not require any additional staff mechanisms to execute the five Offensive IO tasks. As a final analysis of the need for an IO Coordination Cell, the following question must be answered: "Does FM 100-6D identify any required IO staff responsibilities that can only be executed by the IO Coordination Cell?" A complete list of the IO Coordination Cell's responsibilities is provided in Appendix C, IO

Coordination Cell Staff Responsibilities. The responsibilities that apply to Offensive IO are:

- Establish IO priorities to accomplish planned objectives.

- Synchronize, coordinate and deconflict Offensive IO to support the commander's concept of the operation.

- Recommend taskings to the G3 for the assets needed to execute IO.

- Coordinate IO input into paragraph 3, Concept of Operation and Coordinating instructions.

- Coordinate intelligence support from the ACE, and nation-level assets."[57]

In an analysis of the tasks to determine which ones are not currently executed by the other staff agencies, the last three tasks (recommend taskings to the G3; coordinate input into OPORDs, and coordinate intelligence support) fall out. They are executed by the primary staff agency for the specific Offensive IO tasks. The first two tasks (designate IO priorities; and synchronize offensive IO) are not specifically designated to a staff agency. Although the primary staff agencies for the individual Offensive IO tasks execute these responsibilities for their specific area, no one is currently designated to consider the overall IO mission for priorities and synchronization.

Before making a final analysis on these two responsibilities, first consider the individual responsibilities established in FM 100-6D for the six members of the IO Coordination Cell. Table 2.2, Division IO Section with Individual Mission/ Responsibilities from chapter two is copied on the next page for easy reference.

The IO Targeting Officer, designated an Army major, is the IO representative on the division targeting board and at targeting meetings. However, the Offensive IO tasks

that normally require participation at the targeting meeting - PSYOP, EW, and operations for physical destruction - are already represented by their primary staff agency. Military deception is represented as required based on the overall deception plan, and CA can be represented as necessary based on the civilian situation. The IO Targeting Officer does not bring any additional expertise to the targeting meeting, although he can articulate the Offensive IO priorities if necessary. The IO Current Operations Officer, designated an Army captain, is responsible for coordinating and monitoring execution of IO in the current fight. FM 100-6D envisions him at the DTAC providing linkage back to the IOCOORD. The responsibilities for the individual Offensive IO tasks remain with the primary staff agency, so this officer is primarily a conduit for information.

SECTION PERSONNEL	MISSION(s)
IO Coordinator (IOCOORD), LTC, FA 30	Overall responsible, coordinates directly with the commander, information manager for the division
IO Plans Officer, MAJ, FA 30	Integrates IO planning into the division plan, works in the division G3 plans cell, planning link to the IOCOORD
IO Targeting Officer, MAJ, FA 30	Integrates and coordinates IO targeting with division targeting, direct link to the ACE
IO Current Opns Officer, CPT, FA 30	Coordinates and monitors execution of IO from DIV TAC, the link between the IOCOORD and the current fight
IO NCO, SFC, 11M50	Coordinates activities of the IO section; produces IO products, provides 24 hour IO synchronization
Info Systems Opns Analyst, SFC, 74B50	Direct link to the Div Signal Office (G6) for defensive IO. Provides interface with G6 for automation support.

Table 2.2 (Repeated from page 15). Division IO Section with Individual Missions/Responsibilities.

The IO NCO's primary responsibility is to coordinate the actions of the IO section and assist the IOCOORD. He coordinates administrative support and is designated as the night shift IO representative in the division main. This position does not fulfill any of the specified Offensive IO responsibilities. The Information Systems Operations Analysis NCO is the conduit between the IO Cell and the division G6 for OPSEC and other defensive IO tasks. He does not have any specified Offensive IO responsibilities.

Of these four positions, only two specific Offensive IO responsibilities are clear. First, to articulate IO priorities at the division targeting meetings that are also attended by the primary staff agencies for the Offensive IO tasks. Second is to serve as a conduit for information from the division TAC back to the division IOCOORD. Subjective analysis cannot justify having either an Army major or captain performing these responsibilities, let alone both a major and a captain.

Of the two remaining positions, one is the IO Plans Officer, designated as an Army major. This position is responsible for integrating IO into the overall division planning effort. This job description correlates to the IO staff responsibility from FM 100-6 of "synchronize, coordinate, and deconflict Offensive IO to support the commander's concept of the operation." Similar to other special staff officers, the IO Planner is assigned to the IO Coordination Cell but works in the G3 Plans Section. During division planning for offensive actions, he integrates Offensive IO. However, the analysis above determined that the individual staff sections are already synchronizing and coordinating their actions. The remaining task is to deconflict Offensive IO. The division's G3 as the officer overall responsible for the division's operations is the master arbitrator when necessary. The necessity of an individual solely responsible for deconflicting IO may be necessary for specific operations, but subjectively it is not a full-time position.

The final position in the IO Coordination Cell is the IO Coordinator position which is designated as an Army lieutenant colonel. The remaining IO responsibility from FM 100-6D is 'establish IO priorities to accomplish planned objectives.' This is inherent in the IOCOORD job description from FM 100-6D that includes "responsible for overall

planning, preparing and executing of information operations ... the information manager across all disciplines."[58] This responsibility is not currently designated to anyone on the division staff. Although this task may be necessary to allocate limited resources, again subjectively is not a task requiring a lieutenant colonel's full-time attention. At this point the monograph has identified four IO staff responsibilities that are not performed by current staff mechanisms. The tasks are:

- Articulate IO priorities at the division targeting meetings.

- Serve as a conduit for information from the division TAC to the IOCOORD.

- Deconflict Offensive IO to support the commander's concept of the operation.

- Establish IO priorities to accomplish planned objectives.

It has been determined that each of these tasks alone does not constitute an individual staff officer. The last two tasks are interrelated because the IO priority list is the tool for deconflicting support. The first task, articulating these priorities at the targeting meeting, is also a subcomponent of establishing the priority list. Therefore, these four tasks can be restated as the follows:

- Establish and publish Offensive IO priorities to deconflict IO missions and accomplish the division commander's intent.

- Battletrack Offensive IO across the division.

These two tasks must be conducted to effectively execute Offensive IO. However, the heavy division does not require a six soldier Information Operations Coordination Cell to conduct these tasks. Chapter six, Conclusion and Recommendations, provides two alternatives to the six soldier IO Coordination Cell that can perform the necessary staff responsibilities without wasted manpower.

Conclusion and Recommendations

Conclusion

This monograph analyzed the need for the Information Operations Coordination Cell in a heavy division to conduct Offensive IO during an offensive action. The monograph answered supporting research questions that determined the necessary Offensive IO tasks, the division's Offensive IO capabilities to execute those tasks, and the staff mechanisms necessary to conduct the possible Offensive IO actions. The final conclusion is that there are only two staff mechanisms necessary to conduct Offensive Information Operations that are not currently being conducted by the division staff. The two staff mechanisms are:

- Establish and publish Offensive IO priorities to deconflict IO missions and accomplish the division commander's intent.

- Battletrack Offensive IO across the division.

The monograph determined that a six soldier IO Coordination Cell is not necessary to execute these two staff responsibilities.

Recommendations

While this answers the basic research question, an additional question worth some consideration is "Who should execute these Offensive IO staff tasks?" This topic is worth more detailed research and analysis, but based on the initial research conducted for this monograph, two possible recommendations are offered. One alternative is to establish a special staff officer, the IO Coordinator, without the additional five soldier staff. The officer would retain the job description listed in FM 100-6D.[59] This staff officer would work closely with the division G3 section for physical destruction, military

deception, and EW issues, and with the PSYOP officer and G5 for their areas. His overarching responsibility would be to prioritize and deconflict IO actions. A limitation of this recommendation is the lack of administrative support for the IOCOORD.

An alternative recommendation is to establish a division IO officer within the division's G3 section. This officer would function much like the current special staff officers in the G3 section (examples are the DFSCOORD, Special Operations Coordinator (SOCOORD) military deception officer and EW officer) providing expertise on Offensive IO actions through recommendations to the division G3. He would execute the two Offensive IO tasks (establish Offensive IO priorities to deconflict IO missions and battletrack Offensive IO) but as part of the G3 section rather than as a division special staff. The advantage of this recommendation is that the division G3 section already has the administrative support. A possibly perceived disadvantage is that the IO officer would not have the visibility of a special staff officer. However, another viewpoint might argue that the G3 is currently responsible for all division operations and IO should not be handled independent of other operations.

This monograph recommends that one IO officer should be located on the heavy division staff to conduct Offensive IO staff actions to support the division in the offense. Additional research is required to determine if the IO Coordination Cell is necessary for Offensive IO in the other three military actions - defense, support and stability. Research is also necessary to determine if the Cell is necessary for Defensive IO across all four military actions. A possible solution during military actions that require more IO support is to augment the one division IO officer with IO experts from the Department of the Army Land Information Warfare Office (LIWA) or other agencies. This

recommendation, currently in effect with Task Force Eagle in Bosnia Herzegovina, requires additional research before becoming Army doctrine.

Appendix A, G3 Staff Responsibilities for Operations and Planning.

Source: FM 101-5, Staff Organization and Operations, dated 31 May 1997, Chapter 4, Staff Responsibilities And Duties, pages 4-12 - 4-13.

The G3 is the principal staff officer for all matters concerning operations and plans. Within operations and plans, the G3 is responsible for the following specific tasks:

- Preparing, coordinating, authenticating, publishing, and distributing the command SOP, OPLANs, OPORDs, fragmentary orders (FRAGOs), and warning orders (WARNOs) to which other staff sections contribute.

- Planning, coordinating and supervising exercises.

- Participating in targeting meetings.

- Reviewing plans and orders of subordinate units.

- Synchronizing tactical operations with all staff sections.

- Reviewing entire OPLANs and OPORDs for synchronization and completeness.

- Monitoring the battle.

- Ensuring necessary combat support (CS) requirements are provided when and where required.

- Coordinating with the G5 on using tactical forces to establish civil governments.

- Coordinating with the G2 to write the reconnaissance and surveillance annex, which includes tasking units with available assets, to collect the commander's priority intelligence requirements (CCIR).

- Recommending IR to the G2

- Integrating fire support into all operations.

- Planning troop movement, including route selection, priority of movement, timing, providing security, bivouacking, quartering, staging, and preparing of movement order.

- Recommending priority for allocating critical command resources, such as, but not limited to:

Time (available planning time)

Ammunition basic loads and the controlled supply rate (CSR) of ammunition.

Personnel and equipment replacements.

Electronic frequencies and secure key lists.

- Developing ammunition required supply rate (RSR) in coordination with the G2 and G4.

- Requisitioning replacement units through operational channels.

- Establishing criteria for reconstitution operations.

- Recommending use of resources to accomplish both maneuver and support, including resources required for deception purposes.

- Coordinating and directing terrain management (overall ground manager).

- Determining combat service support (CSS) resource requirements in coordination with the G1 and G4.

- Participating in course of action and decision support template (DST) development with the G2 and FSCOORD.

- Coordinating with ENCOORD, G2, G5 and surgeon to establish environmental

vulnerability protection levels.

- Furnishing priorities for allocation of personnel and critical weapon systems replacement to combat units.

- Recommending the general location of command posts.

- Recommending task organization and assigning missions to subordinate elements, which includes:

Developing, maintaining, and revising the troop list.

Organizing and equipping units, include estimating the numbers and types of units to be organized and the priority for phasing in or replacing personnel and equipment.

Assigning, attaching, and detaching units, detachments, or teams.

Receiving units, detachments, or teams, including orienting, training, and reorganizing them as necessary.

- Coordinating with the G1 (CPO) civilian personnel involvement in tactical operations.

Appendix B, G5 Staff Responsibilities.

Source: FM 101-5, Staff Organization and Operations, dated 31 May 1997, Chapter 4, Staff Responsibilities And Duties, pages 4-15 - 4-16.

The areas and activities that are the specific responsibility of the G5 are:

- Advising the commander on the civilian impact on military operations.

- Advising the commander on his legal and moral obligations concerning the impact of military operation s on the local populace for both the short and long term.

- Minimizing civilian interference with combat operations, to include dislocated civilian operations, curfews, and movement restrictions.

- Advising the commander on the employment of other military units that can perform CMO missions.

- Establishing and operating a civil-military operations center (CMOC) to maintain liaison with and coordinate the operations of other US government agencies; host nation civil and military authorities; and nongovernmental, private voluntary, and international organizations in the area of operations.

- Planning positive and continuous community relations programs to gain and maintain public understanding and good will, and to support military operations.

- Coordinating with the SJA concerning advice to the commander on rules of engagement for dealing with civilians in the area of operations.

- Providing recommended CMO-related IR and EEFI to the G2.

- Coordinating with the G3 (FSCOORD) on protected targets.

- Providing the G2 operational information gained form civilians in the area of operations.

- Coordinating with the G3 (PSYOP) on trends in public opinion.

- Coordinating with the G1 (surgeon) on the military use of civilian military facilities, materials, and supplies.

- Assisting the G1 with coordination for local labor resources.

- Coordinating with the PAO and G3 (PSYOP) to ensure disseminated information is not contradictory.

- Coordinating with the PAO on supervising public information media under civil control.

- Providing instruction to units or officials and the population in identifying, planning, and implementing programs to support the civilian populations and strengthen the host nation internal defense and development.

- Identifying and assisting the G6 with coordination for military use of local communications systems.

- Providing technical advice and assistance in the reorientation of enemy defectors, EPWs, and civilian internees and detainees.

- Participating in targeting meetings.

- Coordinating with the G3 (PM) the planning of the control of civilian traffic in the area of operations.

- Assisting the G3 with information operations.

- Identifying and assisting the G4 with coordination for facilities, supplies, and other material resources available from the local civil sector to support military

operations.

- Coordinating with the G1 and SJA in establishing off-limits areas and establishments.

- Coordinating with the SJA on civilian claims against the government.

- Staff planning and supervision over -

Attached CA units.

Military support to civil defense and civic action projects.

Protection of culturally significant sites.

Humanitarian civil assistance and disaster relief.

Noncombatant evacuation operations (NEO).

Emergency food, shelter, clothing, and fuel for local civilians.

Public order and safety as it applies to military operations.

Appendix C, IO Coordination Cell Staff Responsibilities.

Source: FM 100-6, Information Operations: Tactics, Techniques, and Procedures, dated June 1998, page 2-3, Section II, The IO Staff.

In addition to the general staff responsibilities in FM 101-5, the following specific IO actions are taken by the staff:

Establish IO priorities to accomplish planned objectives.

Synchronize, coordinate and deconflict Offensive IO and Defensive IO to support the commander's concept of the operation.

Recommend taskings to the G3 for the assets needed to execute IO.

Coordinate IO input into paragraph 3, Concept of Operation and Coordinating instructions.

Coordinate intelligence support from the ACE, nation-level assets, and Special Technical Operations (STO).

Monitor input into information superiority to create an understanding of the situation as the basis for making decisions.

Ensure solutions are provided to the command to reverse IO vulnerabilities.

ENDNOTES

[1] *The* Army, U.S. Code, Title 10, Section 3062, Subtitle B, Army, Part I, Organization, Chapter 307 (1997).

[2] Franklin C. Spinney, "Genghis John," *U.S. Naval Institute Proceeds*, July 1997, 51,

[3] U.S. Department of the Army, Table of Organization and Equipment (TOE) number 87000A100 for an Armor Division with 5 M1 tank battalions and 4 BFVS battalions, 29 October 1998.

[4] U.S. Department of the Army, FM 100-6, Information Operations: Tactics, Techniques, and Procedures, (Integrated Concept Team Draft), (Washington D.C., Government Printing Office, June 1998), 1-12.

[5] RII defined in FM 100-6, Information Operations: Tactics, Techniques, and Procedures on page 1-10 as :all relevant information of importance to the commander in the exercise of command and control: includes information about friendly forces, the enemy, potential adversaries, neutrals and the operations are to facilitate decision making.

[6] Information Systems defined in FM 100-6, Information Operations: Tactics, Techniques, and Procedures on page 1-10 as: the entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display and disseminate information.

[7] FM 100-6, Information Operations: Tactics, Techniques, and Procedures , 1-10.

[8] Ibid. 4-1.

[9] Special IO is included in the doctrinal definition, however it is beyond the scope of this monograph and will not be discussed. See delimiters for a further explanation.

[10] Defensive IO is defined on page 1-13 of FM 100-6, Information Operations: Tactics, Techniques, and Procedures as "the integration and coordination of policies and procedures, operations, personnel, and technology to protect information and defend information systems. Defensive IO are conducted through information assurance, physical security, OPSEC, counter-deception, PSYOP, counterintelligence, electronic warfare, and special information operations. Defense IO ensures timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes."

[11] Although initially defined in the Office of the Joint Chiefs of Staff Joint Electronic Library's JCS Pub 1-02, Department of Defense Dictionary of Military and Associated Terms dated June 1998, it is also accepted by Army doctrine as the definition for deception. See AR 310-25, Dictionary of United States Army Terms, or FM 90-2, Battlefield Deception, for the same definition with reference back to JCS Pub 1-02.

[12] U.S. Department of the Army, FM 90-2, Battlefield Deception (Washington D.C., Government Printing Office, October 1988), G-4.

[13] Discussed in Chapter 6, page 3 of FM 100-6, Information Operations: Tactics, Techniques, and Procedures. Also established in FM 90-2, Battlefield Deception, in Chapter 3.

[14] Chapter 4, Deception Planning Considerations, of FM 90-2, Battlefield Deception describes three techniques of deception planning - commanders only, close hold, and ad hoc staff. If the division commander chooses to use the commander only technique, the division operations officer within the G3 shop may be excluded from that specific plan. However, IAW FM 90-2 the division operations officer is the primary staff officer for deception planning because: deceptions are as much a function of operations as a real plan; they are part of the operational scheme chosen to accomplish a mission; the G3 section drives the other staff section estimates and annex development processes; the G3 section must deconflict all aspects of the deception plan with both the deception plan itself and the real plan; and fragmentary orders are published by the G3 section.

[15] U.S. Department of the Army, FM 34-10, Division Intelligence and Electronic Warfare Operations (Washington D.C., Government Printing Office, November 1986), *iv.*.

[16] U.S. Department of the Army, FM 34-1, Intelligence and Electronic Warfare Operations (Washington D.C., Government Printing Office, 28 September 1992) 2-20.

[17] CA mission as defined on page 1-1 of FM 41-10, Civil Affairs Operations, dated 11 January 1993.

[18] Ibid. 4-7.

[19] Office of the Joint Chiefs of Staff Joint Electronic Library, JP 1-02, Department of Defense

Dictionary of Military and Associated Terms, (Washington D.C., June 1998), 30.

[20] Martin C. Libicki, What is Information Warfare?, (Washington DC: Center for Advanced Concepts and Technology, Institute for National Strategic Studies. August 1995) 37.

[21] An example is the war scenarios planned by the Intelligence and Security Command as outlined in the *Time* Magazine cover article "Onward Cyber Soldiers", by Douglas Waller Washington, dated August 21, 1995. Futuristic CNA plans included incapacitating the enemy's telephone networks with a computer virus; computer logic bombs set to activate at prescribed times that destroy the control routers for rail lines; misinformation interjected on enemy C2 nets to disorient troop commanders; and emptying the adversary's bank accounts to render him broke.

[22] The liberation of Kuwait is defined in FM 100-5, Operations (Revised Final Draft) as "an offense, with complementary defense, stability and support mission." U.S. Department of the Army, FM 100-5, Operations (Revised Final Draft) (Washington D.C., Government Printing Office, 19 June 1998) 2-22.

[23] U.S. Department of the Army, FM 100-40, Tactics, (Draft) (Washington D.C., Government Printing Office, 3 October 1998) 2-8.

[24] U.S. Department of the Army, FM 101-5-1, Operational Terms and Graphics, (Washington D.C., Government Printing Office, 30 September 1997) 1-113.

[25] FM 100-5, Operations, (Revised Final Draft) 2-24.

[26] Definitions from FM 100-5 Operations, (Revised Final Draft). Defensive actions (page 2-27) are those that resist, defeat or destroy an enemy attack. Although these actions may achieve an acceptable end, they cannot achieve a final decision unless combined with an offensive action. Stability actions (page 2-30) apply military power to influence the political and civil environment in a given region. They include developmental and coercive actions. Stability operations have several purposes that include: deter or thwart aggression, maintain or restore order, and encouraging a weak or faltering government. Because of their nature, stability operations are often precursors or postscripts to other military actions. Support actions (page 2-31) provide supplies and services to designated groups in order to relieve suffering and help civil authorities respond to crisis. Support operations may be either domestic or overseas. Support actions may be independent or may complement the other military actions.

[27] Page 23 of the translation by T.W. Kuo, dated 1989, and titled Sun Tzu: Manual for War. T.W. Kuo, Sun Tzu: Manual for War, (Chicago, Illinois: Alti Press, 1989). Samuel G. Griffith in his book titled Sun Tzu, The Art of War has similar translation such as "know the enemy and know yourself; in a hundred battles you will never be in peril" on page 84, or when referring to spies "secret operations are essential in war, upon them the army relies to make its ever y move" on page 149. Samuel G. Griffith, Sun Tzu, The Art of War, (London, England: Oxford University Press, 1963).

[28] Thomas R. Phillips, BG, ed., *Frederick the Great*, in Roots of Strategy - The 5 Greatest Military Classics of All Time, (Harrisburg, Pennsylvania, Stackpole Books, March 1985) 354.

[29] Thomas R. Phillips, BG, ed., *Napoleon*, in Roots of Strategy - The 5 Greatest Military Classics of All Time, (Harrisburg, Pennsylvania, Stackpole Books, March 1985) 433.

[30] J.F.C. Fuller, The Foundations of the Science of War, (NEED PUBLISHER INFO) 314.

[31] Page 2-3, of FM 100-5, Operations, dated June 1993. This is the current version of FM 100-5 that is expected to be replaced by the draft FM 100-5 dated 19 June 1998. The current version is used here to show the continuity of infiltrating the enemy's decision cycle as part of the doctrine and practices of warfare. U.S. Department of the Army, FM 100-5, Operations, (Washington D.C., Government Printing Office, June 1993) 2-3.

[32] FM 100-5, Operations, (Revised Final Draft) 6-7.

[33] COL Boyd never published his OODA loop theory but included it in a 13 hour briefing titled "Discourse on Winning and Losing" that was presented throughout the Department of Defense. His theories and research have been captured in several articles to include: "Genghis John" by Franklin C. Spinney that was published in *The US Naval Institute's Proceedings,* in July 1997 just after COL Boyd's death. Spinney worked with COL Boyd for over 23 years. Additionally, MAJ David S. Fadok, USAF includes a detailed analysis of Boyd's OODA loop theory in his School of Advanced Air Power theses titled *John Boyd and John Warden, Air Power's Quest for Strategic Paralysis*, dated February 1995 and published by the Air University Press at Maxwell Air Force Base, Alabama.

[34] David S. Fadok, *John Boyd and John Warden, Air Power's Quest for Strategic Paralysis*, (Maxwell Air

Force Base, Alabama: Air University Press, February 1995) 16.

[35] FM 34-10, Division Intelligence and Electronic Warfare Operations, 5-9

[36] FM 100-40, Tactics (Final Draft), 4-1.

[37] According to FM 41-10, Civil Affairs Operations, dated 11 January 1993, page 6-2, Title 10 of the US Code prohibits intelligence collection by personnel not authorized. Because of their unique role within the local populous CA personnel are not authorized intelligence collectors. They must not either conduct intelligence collection nor give the appearance of intelligence collection. CA personnel must not be included in the unit's information gathering plan. However, CA personnel can and do provide reports on information that they receive in the process of executing their responsibilities. They can provide maps, files of newspaper accounts, government documents, personal data to include: technical skills, religious affiliations, propensity for housing enemy personnel, potential recruits for intelligence, SF, or PSYOP personnel etc.

[38] U.S. Department of the Army, FM 46-1, Public Affairs Operations, (Washington D.C., Government Printing Office, May 1997) 32.

[39] U.S. Department of the Army, FM 71-100, Division Operations, (Washington D.C., Government Printing Office, 28 August 1996) 1-4. This description also applies to US mechanized forces, however the reference to mechanized forces was deleted because the monograph's focus is on the armored division. The deletion is not intended to minimize the importance and effectiveness of mechanized forces.

[40] FM 90-2, Battlefield Deception, 5-10.

[41] U.S. Department of the Army, FM 33-1-1, Psychological Operations Techniques and Procedures, (Washington D.C., Government Printing Office, 5 May 1994) I-9.

[42] U.S. Department of the Army, Table of Organization and Equipment (TOE) number 87000A100 for an Armor Division with 5 M1 tank battalions and 4 BFVS battalions, 29 October 1998.

[43] U.S. Department of the Army, TOE number 34395A000, MI Bn (CEWI) Heavy Division, Recapitulation of equipment, dated 29 October 1998, a supporting document for TOE number 87000A100, Armor Division with 5 M1 tank battalions and 4 BFVS battalions, dated 29 October 1998.

[44] FM 71-100, Division Operations, 2-20.

[45] Ibid. 4-7.

[46] U.S. Department of the Army, FM 6-20-30, TTPs for Fire Support for Corps and Division Operations, (Washington D.C., Government Printing Office, 18 October 1989) B-1, Fire Support Planning Factors, and Chapter 4, Section V. Deep Operations.

[47] U.S. Department of the Army, FM 101-5, Staff Organization and Operations, (Washington D.C., Government Printing Office, 31 May 1997) 4-25.

[48] U.S. Department of the Army, Table of Organization and Equipment (TOE) number 87000A100 for an Armor Division with 5 M1 tank battalions and 4 BFVS battalions, 29 October 1998..

[49] FM 101-5, Staff Organization and Operations, 4-27 through 4-28.

[50] FM 33-2, page 3-22

[51] FM 101-5, Staff Organizations and Operations 4-25.

[52] FM 71-100, Division Operations, 2-14.

[53] FM 33-1, page 3-3

[54] U.S. Department of the Army, FM 34-1, Intelligence and Electronic Operations, 2-21.

[55] FM 71-100, Division Operations, 2-23.

[56] Original source is FM 101-5, Staff Organization and Operations, Chapter 4, Staff Responsibilities And Duties, pages 4-15 - 4-16. For easy reference, all of the CA Staff Responsibilities are also listed in Appendix B, G5 Staff Responsibilities to this monograph.

[57] FM 100-6, Information Operations: Tactics, Techniques, and Procedures, (Integrated Concept Team Draft), 2-3

[58] Ibid., 2-4.

[59] This job description is discussed in Chapter 5 of the monograph. The exact verbiage from FM 100-6, Information Operations: Tactics, Techniques, and Procedures, (Integrated Concept Team Draft) is "LTC, FA 30, responsible for overall planning, preparing, and executing of information operations; works directly for the chief of staff; coordinates directly with the commander and coordinating staff principles - primarily the G2, G3, G5, and G6 - and selected special staff organizations (leads the IO cell - this responsibility is deleted for the recommended solution because the IO cell no longer exists). He is the info manager across all disciplines to all staff elements/brigades. He writesIO annexes to OPLAN/OPORDs.