Incidental Paper

Unholy Matrimony: The Marriage of Operations and Intelligence in C^3I

Stephen W. Sutton

Program on Information Resources Policy

Harvard University

Center for Information Policy Research

Cambridge, Massachusetts

An incidental paper of the Program on Information Resources Policy.

Unholy Matrimony: The Marriage of Operations and Intelligence in C^3I

Stephen W. Sutton
August 1990, I-90-2

Colonel Stephen W. Sutton completed this study while assigned as the 1987-1988 Air Force Research Associate at the Program on Information Resources Policy at Harvard University. Sutton's current assignment is Assistant Deputy Chief of Staff, Plans, at the Air Force's Electronic Security Command, Kelly Air Force Base, Texas.

Printing 5 4 3 2 1

August 1990

PROGRAM ON INFORMATION RESOURCES POLICY

Harvard University **Center for Information Policy Research**

Affiliates

ABRH Consulting
Action for Children's Television
American Newspaper Publishers Association
American Telephone & Telegraph Co.
Ameritech Publishing
Apple Computer, Inc.
Arthur D. Little, Inc.
Auerbach Publishers Inc.
Bell Atlantic
Bell Canada
BellSouth Corporation
Boice Dunham Group Inc.
Bull, S.A. (France)
Centel Corporation
Chronicle Broadcasting Company
CMC Limited (India)
Commission of the European Communities
Communications Workers of America
Computer & Communications Industry Assoc.
COMSAT
Data America Corp.
Dialog Information Services, Inc.
Digital Equipment Corp.
Dow Jones & Co., Inc.
France Telecom
Gartner Group, Inc.
GTE Corporation
Hitachi Research Institute (Japan)
Honeywell, Inc.
IBM Corp.
Information Gatekeepers, Inc.
Information Industry Association
International Data Corp.
International Resource Development, Inc.
Invoco AB Gunnar Bergvall (Sweden)
I.T. Direction Ltd. (UK)
Knowledge Industry Publications, Inc.
Lee Enterprises, Inc.
John and Mary R. Markle Foundation
MCI Telecommunications, Inc.
Mead Data Central
MITRE Corp.
National Telephone Cooperative Assoc.
The New York Times Co.
NEC Corp. (Japan)
Nippon Telegraph & Telephone Corp. (Japan)
Northern Telecom Ltd. (Canada)
Nova Systems Inc.
NYNEX
Ing. C. Olivetti & Co., S.p.A.
OTC Limited (Australia)
Pacific Telesis Group
Public Agenda Foundation
Research Institute of Telecommunications and Economics (Japan)
RESEAU (Italy)
Revista Nacional de Telematica (Brazil)
Salomon Brothers
Scaife Family Charitable Trusts
SEAT S.P.A. (Italy)
Southern New England Telecommunications Corp.
State of California Public Utilities Commission
State of Minnesota Funding
TEKNIBANK S.p.A. (Italy)
Telecom Australia
Telecommunications Research Action Center (TRAC)
Tele/Scope Networks, Inc.
Third Class Mail Association
Times Mirror Co.
Tribune Company
United States Government:
- Department of Commerce
  - National Telecommunications and Information Administration
- Department of Defense
  - National Defense University
- Department of Health and Human Services
  - National Library of Medicine
- Department of State
  - Office of Communications
- Federal Communications Commission
- General Services Administration
- National Aeronautics and Space Administration
- National Security Agency
- U.S. General Accounting Office
- United States Postal Rate Commission

United Telecommunications, Inc.
US West
Williams Telecommunications
Wolters Kluwer

Disclaimer

The views, opinions and/or conclusions in this paper are those of the author and should not be construed as the position of a Department of Defense, U.S. Air Force, or any other governmental office.

Table of Contents

List of Tables

Executive Summary

• Command, Control, Communications, and Intelligence (C^3I) is strongly supported by national strategy. C^3I's high priority is reflected in the portion of national budget allocated to it.

• Integration of intelligence and command and control serves as a "force multiplier" in military operations. With numerical inferiority facing U.S. forces in the future, the C^3I "marriage" becomes even more significant.

• C^3I is often considered as a homogeneous grouping of functions. The intelligence community and the military are made up of fragmented groups of organizations. Each has its own set of priorities. Orchestration of this network presents unique challenges.

• Policy decisions designed to provide the best control and management of intelligence at the "national" level may create problems at other levels in the chain of command. "Resource factors" are related to "owning" of resources, advocacy of programs, and control of the budget. Classification of information forces the proper balance between protecting sources and providing enough information.

• Military doctrine and strategy are developed by the services as the basis for their tactical schemes. C^3I resources required by doctrine and strategy often fall outside either field commander or service span of control leading to the need to share limited national-level assets.

• The view of the intelligence segment of C^3I varies at different levels of government. These range from Congressional concerns with the legal and moral questions of intelligence to budgetary and procedural-information-sharing concerns at other levels.

• C^3I concerns also exist within NATO. With recent INF Treaty developments, attention has been focused on Soviet strategy shifts which could ultimately lead to changes to NATO CC^3I support requirements. Several programs being developed in Europe and the U.S. to support NATO C^3I could be affected.

• Dilemmas arise in integrating intelligence into military command and control decision-making. These are related to resource management, program advocacy, classification and control of information, cost of technology, interoperability, and the equitable sharing of "national" intelligence assets.

The information base for this paper

ends the summer of 1988.

CHAPTER ONE

INTRODUCTION

This study examines various policies affecting the intelligence community[1] of the United States and how they can impact the ability of our military to accomplish its operational taskings. It is intended to serve as an introduction to this subject for use by senior policy makers within government as well as by laymen. The purposes of this report are to

- Improve understanding of the importance of command, control, communications, and intelligence (C^3I) from a strategy perspective.
- Provide a review of the organizational structure of the intelligence community and the military services that must be "married" when forces are employed.
- Discuss some of the more important factors which tend to impede the integration of intelligence information into military operational command and control.
- Review the requirements for intelligence and command and control created by the services' doctrine and strategy. Specifically, we will look at the Army and Air Force doctrine of the AirLand Battle and the Navy's Maritime Strategy. In examining these, we will consider the demands that tactical considerations can place on the need for optimum intelligence to operations linkage.
- Consider the views of the uses of intelligence from various levels of government, such as Congress and the intelligence community.
- Review some of the concerns related to intelligence and its integration into the command and control of theatre forces. As a case in point, we will review one of our major alliance commitments -- NATO -- and some concerns with C^3 and I in that theatre.
- Summarize many of the factors that can impede the integration of intelligence information into military decision making. These include setting priorities for intelligence and command and control systems, the advocacy of these programs, the classification and control of the information itself, the challenges of technology, the question of adequate interoperability, and the achievement of the proper balance of intelligence priorities in supporting both "national" and "tactical" taskings.

1.1 WHAT ARE THE ISSUES?

We tend to consider the subject of C^3I as a "homogeneous" grouping of functions. From the standpoint of force employment, this would be the ideal situation. But in practice, this isn't the way things work. Congressman Charles Rose commented on the "marriage" of the C^3 and I terms:

> Command, Control, Communications, and Intelligence (C^3I) has become a buzzword of the late 1970s and early '80s. Back in 1977 a strange thing happened in the Pentagon: somebody decided "C^3" and the "I" went together. A shotgun marriage at best.[2]

His point serves as a foundation for the discussions of this paper. A number of issues will be looked at more closely. These are related to the purposes of this study and include the following:

- Are the roles of the players in the C^3I communities clearly defined? Factors related to control of resources, program advocacy, fiscal constraints, classification, technology, and others impact the effectiveness of the C^3I marriage.
- Is there a coherent set of policies for dealing with the employment of military force which uses the instruments of intelligence effectively?

When you consider the range of force employment possibilities that exist today, this is no simple task. In the past, it was relatively easy to separate requirements for strategic levels of armed conflict from those directed at the "tactical" level. The "rules" are changing. An "operational" level of war has been introduced into military doctrine. This level "transcends" strategic and tactical employment scenarios. It has been referred to as an action using "military resources to attain strategic goals within a theatre of action."[3] More importantly, operational level thinking creates requirements for intelligence and command and control links which earlier doctrine did not require.

In addition, "national-level" intelligence policy was last formally expressed in the year preceding introduction of this "new" level of war.

Therefore, the operational level of war is not addressed in current national intelligence policy. This leads to new questions related to the allocation of scarce resources, such as the intelligence assets needed to support military operations:

- Are service doctrinal goals achievable in today's policy environment? Has force structure kept pace with doctrine? We will look at the Army and Air Force's AirLand Battle doctrine and review its goals. In doing this, we need to consider the intelligence community's linkage to theatre forces in future program and policy decisions.

- Can service strategy be achieved in the current policy environment? We will look at the Navy's Maritime Strategy and consider the policy demands it places upon the intelligence community and the military establishment.

- Is the importance of intelligence to military operations fully understood at every level of government? We will look at the views of both Congress and the intelligence community about the current C^3I situation.

- Are C^3I concerns the same in the multinational environment? We will consider NATO's C^3I concerns as an example of those found in many multinational alliance situations.

1.2 HOW IS THIS SUBJECT ADDRESSED?

We begin discussion of the C^3 and I marriage with a review later in this chapter of the priority given to the subjects of intelligence and command and control. This priority is expressed in various strategy statements from the president and the Defense Department. How strong is the commitment to these priority statements? Current budget allocations to these mission areas say a great deal about this priority and amplify the "force multiplier" value of C^3I. We will discuss aspects of this in both this and subsequent chapters.

As we move on in chapter 2, we will continue to focus on the purposes of this study and shed light on the issues that impact the C^3I interface. We will begin by briefly reviewing the basic roles that intelligence functions fill. Next, we will review the "intelligence players" -- the various agencies that perform intelligence roles in our

government. We'll consider the "players" who set the priorities for intelligence resources -- who decides what capabilities are bought and how they are used. Then we'll review the organizational framework of our defense establishment in order to better understand the framework to which intelligence resources must be "married." Finally, we will review three sets of factors that tend to impede the integration of intelligence into operational command and control. These include policy factors, such as who "controls" intelligence assets needed for theatre military operations; resource factors, such as costs, tradeoffs, budget control, and priorities that can prevent obtaining capabilities needed for the support of military operations; and classification factors that can provide procedural frustration and impede the best intelligence to operation integration.

In chapter 3 we will consider four major topics related to both the purposes and issues of this study. The first of these is the Army and Air Force's AirLand Battle doctrine. We will briefly review its evolution and discuss its demands. We will look at some concerns with the doctrine from within the Army -- specifically, has force structure and policy for C^3I kept pace with the doctrine? Army force doctrine says, "we're going to fight the AirLand Battle" while its organization, training, and force structure are still set up based upon earlier "how to fight" schemes.

Next, we will look at the Navy's Maritime Strategy and the requirements it places for integration of intelligence into naval operations. The concerns here are more global in perspective and again raise the question of control of intelligence assets. Specifically, with the "offensive" orientation of the Maritime Strategy, the availability of "national" intelligence may be needed to give the strategy a chance for success. Control of these assets is fragmented among the many agencies of the services and the national intelligence community, which are outlined in chapter 2.

Also in chapter 3, we will look at other perspectives of intelligence from different vantage points of our government. Views of Congress, for

example, have largely centered on the legitimacy of intelligence operations. While important, these have not contributed to enhancement of intelligence support for military operations. Other concerns from Congress with C^3I have centered on the cost, complexity, lack of coordinated advocacy, and the classification of the many systems that contribute to these capabilities.

Finally, in chapter 3, we will address C^3 and I from the perspective of a multinational example -- NATO. There are many defense-related concerns in Europe. One of the most basic of these is the INF Treaty's impact on future Soviet strategy in Europe. Changes in Soviet strategy could lead to changes in NATO's response. Strategy shifts would influence NATO doctrine (including the U.S. AirLand Battle portion). Other NATO concerns discussed in this chapter are related to the priority (and commitment) given to intelligence by some NATO member nations. The U.S. and United Kingdom, for example, have shared close ties in intelligence operations going back to World War II. Other NATO countries, such as West Germany (again related to the war experience), view intelligence differently and do not necessarily commit a similar share of resources. Finally, in chapter 3, we will discuss some systems being developed by various NATO and Western European countries that promise to enhance Allied C^3 and I capabilities in Europe. The discussions of this portion of chapter 3 point out the variety of strategy, multinational commitment, and resource factors that can complicate the C^3I equation.

In the final chapter of this paper, we will review a number of "dilemmas" that tie together the various related topics discussed throughout this paper. All of these tend to impede the marriage of intelligence to command and control in military decision making. All are related to the issues of whether C^3I roles are well-defined and whether a coherent set of C^3I policies exists. Discussion in this chapter touches upon the question of resources and advocacy for C^3I programs. Different views of intelligence priority from Congress, from within the intelligence community, and from within the military itself

are discussed. Gaining consolidated advocacy in such a fragmented bureaucracy is difficult.

Other dilemmas discussed include those created by technology (whether an enhanced "capability" promised by a particular system is worth the price), interoperability (whether allies and their systems can "talk" to each other), and commitment of "national" intelligence assets for "tactical" uses (whether there is enough available and how it should be shared).

Before moving on to the topics outlined above, let's review the basis for these discussions of C^3I and the priorities with which they are held within our government.

1.3 WHAT IS THIS C^3I ALL ABOUT?

Since World War II, both the intelligence community and the military of the U.S. have grown and developed. Organizational development has occurred through both a series of independent events and as a result of an explosion of technological capability. Both the intelligence community and the military serve the "national interest." At times, this service is carried out through a coordinated effort. In other situations, they perform service independently. How well-orchestrated is the intelligence and operations "marriage" in the context of military operations? The answer to this question can spell the difference between victory and defeat in military operations. According to Lt. Gen. John Cushman

> We seek an accurate perception of the reality of the battlefield. The enemy seeks to disorient us, to confuse us with deception, to distort what we perceive, to confront us with alarming events not foreseen, to keep us behind the situation, so that what we decide is already wrong even before it is decided.[4]

Employment of military force is one option chosen from many alternatives by national leadership. When the use of military force is

decided upon, its efficient use is essential to insure accomplishment of national objectives while minimizing friendly losses. Many factors influence the success of military force employment. Consider two of the more important of these -- avoiding surprise, and coordinating "friendly" activities.

One force employment consideration is the avoidance of surprise. The importance of surprise (or its avoidance, depending on one's perspective) shouldn't be underestimated. When it has been, the results have often been disastrous. Few in the U.S. will forget the impact of use of surprise by the Japanese at Pearl Harbor. Author Richard K. Betts comments on surprise and its importance: "[S]urprise occurs to the degree that the victim does not appreciate whether, when, where, or how the adversary will strike."[5]

Surprise can take many forms. According to Betts, surprise can be political, strategic, or tactical in nature.[6] There are many ways of reducing the surprise factor. As technology has evolved, so has the U.S. structure for dealing with "surprise avoidance." In the next chapter, we will look at the "surprise avoidance" or intelligence institutions available to support both national leadership and the military. This community exists to deal with the political, strategic, and tactical elements of surprise.

A second major consideration in employing military force is the coordination of friendly force activity once the employment decision has been made. Since the mid-1960s, a great deal of attention has been given to this and the intelligence areas. An entirely new vernacular has evolved to describe these subjects. The terminology applied to force employment coordination became command and control (C^2). Then it was expanded to command, control, and communications (C^3). Finally, the term was expanded even further to include the intelligence function (C^3I).

C^3I can mean many things to many people. To most military commanders, it is the function of *controlling* the employment of military force through the transmission of *command* direction using some means of *communications* linking various systems with which the command decision process is accomplished. Ideally, all of this is done while considering any and all available *intelligence* information.

1.4 WHY IS ALL OF THIS IMPORTANT?

National leadership from the president down formally express their priorities for national security. Let us review a number of national security priority statements in order to establish a framework for evaluating the relative priority of C^3I.

The Goldwater-Nichols DOD Reorganization Act of 1986 established, among other things, a requirement for the president to present to Congress each year "a comprehensive report on the national security strategy of the United States."[7] In the first of these reports, the president established the priority given to C^3I as a segment of the nation's Strategic Modernization Program:

> Current elements of that program (the Strategic Modernization Program), which remains our highest defense priority, include . . . [i]mproved strategic command, control and communications, to ensure timely warning of attack and an assured means of passing retaliatory orders to our strategic forces.[8]

C^3I is also mentioned in the report as a "key" element among the conventional force modernization programs:

> Improvements in C^3I are of continuing high priority in order to strengthen the ability to employ our conventional forces to their fullest.[9]

The priority of C^3I outlined in the president's national strategy is also mentioned in priority statements of the Joint Chiefs of Staff (JCS) and the military services. The JCS's priority for C^3I is expressed in the statement of U.S. Military Posture for FY 1987 in the following ways:

> Command and control is imperative to the successful employment and most effective use of our military forces. . . .
>
> * * *
>
> US military strategy depends heavily on accurate and timely intelligence for warning and effective employment of military forces. Such intelligence increases the likelihood that forward-deployed and reinforcing forces will deter conflict or defend successfully, and maximizes the potential of modern weapons systems.[10]

The military services also recognize the importance of C^3I to national security. Representative among these are the views expressed by Air Force leadership:

> A composite of many capabilities is needed to meet this (the Soviet) challenge: fighter and reconnaissance aircraft, electronic combat forces, special operations forces, strategic and theatre airlift, specialized command and control aircraft, the conventional combat capability of our strategic bombers, stocks of modern munitions to provide accuracy and lethality, and a modern command, control, communications and intelligence (C^3I) system for the efficient, flexible employment of combat forces in all theatres.[11]

Another factor amplifies the relative importance of C^3I -- the persistent pressure for the application from fiscal constraints in planning for military force structuring and employment. The Goldwater-Nichols Bill, for example, now requires the president and the secretary of defense through the chairman of the Joint Chiefs of Staff to exercise fiscal restraint by

> preparing strategic plans, including plans which conform with the resource levels projected by the Secretary of Defense to be available for the period of time for which the plans are to be effective.[12]

Resource levels available for defense in the next few years are not likely to increase. In fact, many analysts forecast defense outlays to decrease in the years ahead. In mid-1987, the Electronic Industries Association (EIA) released an estimate "that defense spending by FY92 is expected to shrink to the levels of the mid-1970s, at which point increases of 1% would return."[13] This fiscal outlook becomes even more relevant when you consider the comparative force levels of the U.S. in relation to the Soviet Union.

U.S. military services operate at a numerical disadvantage in many theatres of potential conflict. In NATO, allied forces possess 90 division equivalents (including the "rapidly deployable" forces whose equipment is in place in Europe). Warsaw Pact forces total 133 division equivalents. Individual weapons systems comparisons are no more favorable. The Warsaw Pact forces hold favorable ratios in the numbers of tanks (32,000 to 19,600), armored personnel carriers (38,000 to 32,850), attack helicopters (960 to 650), antitank weapons (18,000 to 13,370), and artillery (23,000 to 14,200) and continue to produce these weapons at a rate faster than the NATO forces.[14]

Strategic force ratios are no better. The Soviets hold an advantage in the number of ICBM launchers and reentry vehicles, nuclear ballistic submarines, and long range bombers.[15] When the fiscal constraints outlined earlier are considered, these force ratios are not going to change.

What does all of this have to do with C^3I? The answer is -- a great deal. "Force multipliers" such as C^3I become even more important in this environment of unfavorable force ratios and fiscal constraints. Therefore, it's important to try to gain the maximum utility from the forces which are available. C^3I can help make this happen. It is one of the few hopes that can tip the balance in our favor.

As we move on the remaining chapters of this paper, it is important to keep the strategy and force structure considerations outlined above in mind. They serve as the foundation for much of the intelligence and command and control policy and program discussions which follow.

NOTES

1. The term "intelligence community" is taken from *Executive Order 12333* and will be discussed at greater length in subsequent chapters.

2. Charles Rose, "Congress and C^3I," *Seminar on Command, Control, Communications, and Intelligence: Guest Presentations, Spring 1981* (Cambridge, Mass.: Program on Information Resources Policy, Harvard Univ., 1981), p. 169.

3. Field Manual 100-5, *Operations*, Headquarters Department of the Army, Washington, D.C., 20 August 1982, p. 2-3.

4. Lt. Gen. John H. Cushman, *Command and Control of Theatre Forces: Adequacy* (Washington, D.C.: AFCEA Press, 1985), p. 2-58.

5. Richard K. Betts, *Surprise Attack*, The Brookings Institute, Washington, D.C., 1982, p. 4.

6. Ibid., pp. 4-5.

7. P.L. 99-433, *Goldwater-Nichols DOD Reorganization Act of 1986*, 100 STAT. 1075.

8. *National Security Strategy of the United States*, The White House, January 1987, p. 23.

9. Ibid., p. 38.

10. *United States Military Posture for 1987*, Organization of the Joint Chiefs of Staff, Pentagon, Washington, D.C., 1987, p. 9.

11. *Air Force Issues Book*, Headquarters, United States Air Force, Pentagon, Washington, D.C., Spring 1987, p. 3-1.

12. P.L. 99-433, *Goldwater-Nichols DOD Reorganization Act of 1986*, 100 STAT. 1007.

13. Daniel J. Marcus, "Analysts Predict Decade of Tight Defense Budgets," *Defense News* (12 October 1987) 4.

14. For Force structure comparisons, see *Soviet Military Power*, Department of Defense, US Government Printing Office, 1987, p. 93. For comparative production statistics, see p. 122.

15. Ibid., pp. 29-39.

CHAPTER TWO

THE PLAYERS

This paper is devoted to an examination of policies governing the U.S. intelligence community and how these policies impact the operational application of U.S. military force. As we said in the introductory chapter, we will begin by reviewing the roles filled by intelligence in supporting national strategy, surveying the organizations which contribute to the "marriage" of intelligence activities and military operations, and discussing three important factors which can influence the integration of intelligence into military operations -- policy, resources, and classification.

Many "players" support the C^3I process. One segment conducts intelligence activities. Another group is tasked with military force employment. When considering military force projection, one would like to think of these components of our national security infrastructure as a "well oiled machine" driven by a single command, control, communications, and intelligence (C^3I) "system" poised to optimize force employment. This is not the case. C^3I of our military is not that simple or clearly defined. Instead, there is a maze of players with varying priorities, mission taskings, interests, and policies driving their activities. In this chapter, we will review the organizational framework of these players as the background for later discussion.

2.1 HOW DID WE GET HERE?

The national intelligence community and the military command structure of the United States as we know them today share a common beginning. In the period following the conclusion of World War II, U.S. leaders had the opportunity to "invent a new wheel" in order to correct the problems that existed during the war with organizational structures, functional responsibilities, and mission taskings of both our national intelligence agencies and military forces. With the war over, these adjustments could be addressed with the nation no longer engaged in a

shooting war and with the wisdom gained from the successes and failures of the war fresh in everyone's mind. The National Security Act of 1947 is the policy document that resulted from this reform effort.

Within the military, there were major changes generated by the National Security Act of 1947. The Joint Chiefs of Staff were created as the senior military advisory group for the president. The Air Force became a separate service. The position of secretary of defense was created to serve as head of the "National Military Establishment." This was done in an attempt to resolve some of the rivalry problems that had plagued the services throughout the years of the war. (The Defense Department wasn't established until the National Security Act was amended in 1949.)

The National Security Council was also created at this time. It was set up to act as an advisory body to the president in orchestrating political and military actions undertaken in support of national security objectives.

This same legislative act, along with the Central Intelligence Agency Act of 1949, provided the framework for a portion of today's U.S. intelligence community. These acts attempted to address some of the problems experienced during the war with respect to competition among the various agencies and the military in the intelligence field and tried to provide centralization to the collection of intelligence. The position of director of Central Intelligence was created to serve as the single manager of intelligence activities and to enforce priorities assigned to intelligence by national leadership.

The Central Intelligence Agency was created at this time as well. This agency picked up the responsibilities of the earlier office of Strategic Services.

How has this reorganization continued to evolve? How well does the intelligence community's policy structure support military operational doctrine? Do policy makers need to rethink the intelligence objectives

and their relationship to military operations? We will address these and other questions in this and subsequent chapters. Where to begin? First, we will review the roles of intelligence and how these roles support or compliment military operations.

2.2 WHAT ARE THE ROLES OF INTELLIGENCE?

Before proceeding any further, it might prove beneficial to bring all potential readers of this paper to the same level of reference. For this reason, let's take a few moments to review the various roles that intelligence can play in supporting national strategy. Governments have used intelligence for the purpose of conducting foreign policy since biblical times:

> In the old testament one reads that Moses was commanded by God to "spy out the Land of Canaan." Seeking and finding information was crucial to leaders of governments and their armies.[1]

What was true then is no less true today. In the period since the conclusion of World War II, intelligence roles and missions evolved as mission requirements and collection capabilities developed. These activities can be categorized in many different ways but are generally considered as a set of elements consisting of clandestine collection, counterintelligence, analysis and estimates, and covert action.[2] For an expanded discussion of each of these roles, see appendix A of this report.

2.3 WHO PERFORMS THESE ROLES?

In the U.S. government, the above roles are undertaken by various organizations that compose the U.S. "intelligence community." These consist of the CIA, the Department of Treasury, the Department of Commerce, the FBI, the Department of State, the Department of Energy, the NSA, the DIA, and the military services. All have evolved independently and have their own specific taskings. (Appendix B expands

on the mission taskings of the intelligence "players.") Later in this and subsequent chapters, we will discuss some of the turf questions that arise from the fragmented nature of the intelligence community's functional division.

2.4 WHO SETS PRIORITIES?

One question has to come to mind when you consider the size and complexity of the U.S. intelligence community: Who sets the priority on the use of these vast intelligence assets when the "ownership rights" are spread among so many different agencies?

As with many things in our government, the president is the ultimate decision maker on intelligence priorities. The National Security Council, the director of Central Intelligence, the secretary of defense, and the director of the NSA and DIA also play roles in the establishment of intelligence priorities, either through the direct control of an agency's assets or through implied control resulting from the funding allocation stemming from the federal budget process. Appendix C of this report addresses the division of intelligence priority authority among these players in greater detail.

2.5 WHO OPERATES THE MILITARY?

As with the collection of intelligence and the establishment of intelligence priorities, military operations can involve many "players." Each has a set of functional responsibilities.

The president acts as Commander-in-Chief of the Armed Forces. He is advised in various facets of force employment by the National Security Council, the secretary of defense, and the Joint Chiefs of Staff.

Actual employment responsibilities are often delegated to the commanders of the unified and specified commands, depending upon geographical area and mission involved.

The military services are also involved in force employment as well. It is through the services that field commanders are given their strategy or doctrine -- their "how to fight" guidance. Through the services, field commanders are provided the organizational guidelines for their service-component forces. And through the services, much of the training and equipment support for the field commander's forces is received. An expanded discussion of the roles of these "players" in military force employment is provided in appendix D of this report.

2.6 HOW DOES THE CONCEPT OF C^3I FIT TOGETHER?

Now that we have reviewed the players involved in the two "halves" of the force employment business, the intelligence community and the military operational commands, let's return to the discussion which began this chapter. Specifically, how does all of this fit together? We said earlier that we like to think of the intelligence collection and the command and control of forces as a homogeneous grouping of functions. It's implied in the term C^3I itself. After reviewing the various players of the C^3I equation, it becomes apparent that it just isn't that simple. There are many individual "players." Each has "its" own turf. Without trying to oversimplify things, there at least three sets of factors that tend to make a marriage of intelligence and operations more difficult: those derived from policy, driven by resource considerations, or caused by classification of information. Let us consider each separately.

2.6.1 The Policy Factor

The policy guidance in the president's *Executive Order 12333* establishes intelligence community guidelines which are set up (and rightfully so) to serve the top. The intelligence resources are the president's to use in support of the establishment and conduct of national security policy. The agencies governed by this directive are procedurally required to orient their actions to support this end. So what is the problem with this? It boils down to this. A system whose policy guidance is geared to serve the top is not necessarily set up to

support other objectives (such as military operations). In fact, the executive order says that "[a]ctivities to acquire the intelligence required for the planning and conduct of tactical operations by the United States military forces are not included in the National Foreign Intelligence Program."

Because of this policy statement, the National Foreign Intelligence Program falls under the control of the DCI (and perhaps rightfully so) in order to provide the most responsive structure to the president and NSC.

Let's consider an example. What about the position of a military field commander in the European Command? He is tasked with employment of military force in the Fulda Gap of West Germany. His "how to fight" philosophy, developed by his service staff, is one called the AirLand Battle. This doctrine directs him to strike deep, prepare for counter-offensive, and use a combined arms approach making the maximum use of available air power to engage and defeat an enemy which has a decided numerical superiority. This war is to be fought with weapons whose lethality staggers the imagination, with tanks and personnel carriers of impressive speed, and with Mach 2 fighters operating in virtually any weather conditions, either day or night. The speed of the battlefield in question changes the concept of distances that come into the tactical equation. The intelligence and command and control marriage can be a critical one that must be exploited to its full advantage.

It is safe to say that a commander in this situation needs all the intelligence support that can be generated, including some from sources that are considered by current policy to be "national assets." The bottom line is that intelligence policy needs to move forward in order to make this possible.

2.6.2 The Resource Factor

Resource considerations almost always come into any discussion of C^3I. How much is enough? What is the cost? What kinds of tradeoffs are going to have to be considered? Procurement of command and control

systems has been a difficult thing for the military to address for some time. Airplanes, ships, tanks, and missiles are easier to visualize (and to justify with Congress). One can quantify the value of the bomb loads carried by a B-1 or the firepower accuracy of the main gun of an Abrams tank. The value of a command and control system is not really comprehended until one no longer has it. Its value does exist. The same kind of problem also applies to the resourcing of tactical intelligence needs.

Intelligence resource management is further complicated systemically. As mentioned earlier in this chapter, resourcing of intelligence systems is handled through two separate "systems." Intelligence requirements that fall under the "National Foreign Intelligence Program" (the General Defense Intelligence Program and the Special Activities of both the Air Force and Navy are included in this) are managed by the director of Central Intelligence (DCI). The management system used by the DCI in administering this program is called the Capabilities Programming and Budgeting System (CPBS).

Tactical intelligence requirements are managed through a different channel. These fall under the secretary of defense and are managed under the guidance of the DOD's Planning, Programming, and Budgeting System.

These two systems operate independently and on different cycles. Coordination between the two is done at different points in the systems' cycles. The problem of sponsorship of the field commander's operational needs, expressed earlier in the quote from Cushman's book, is only compounded. The situation with intelligence requirements is even more pronounced. The influence of the additional players introduced into this "dual track" scenario exaggerates the distance from the origin of the operational intelligence requirement to its translation into a fielded capability.

Once systems are fielded, the problem of intelligence resource management doesn't end. The question of ownership becomes one of competing priorities. General Lincoln Faurer, a former director of the NSA, addressed the dilemma in this way:

> Let me talk for a moment about SIGINT support to the military commander. A conflict exists between the desire of that commander to control his own assets, and maximum SIGINT support. Every commander will tell you he feels far more confident going into battle with control over both what will fight and what will support him. On the other hand, he currently does not have, and is unlikely to acquire (because of cost limitations) the intelligence wherewithal to fight that battle alone. The assets just can't be made available.[3]

2.6.3 The Classification Factor

The third factor that impacts the C^3I marriage is the availability of the intelligence information itself. This factor is one that depends upon proper balance -- a balance between the protection of information sources, methods, etc. on one hand, and the effective use of the information on the other. This balance must be maintained in order to maximize the utility of the intelligence information.

Intelligence data, as is the case with other sensitive government information, is handled through a classification system. The level of classification is driven by the sensitivity of the information and ranges from unclassified, but sensitive "For Official Use Only" information to the most highly classified "Top Secret -- compartmented" information. In order to obtain access to information of the latter category, the receiver of the information must possess not only the requisite security clearance but also must have the "need to know."

No one can argue that the proper control of sensitive information is essential to the effective completion of a military or intelligence operation. When unauthorized disclosure does occur, the entire activity in question is jeopardized. What must be weighed against this control, however, is access that is sufficient to allow the operation to be

completed. This source of anguish in conducting military operations is particularly difficult in the multinational environment. General Cushman writes from his experiences in Korea:

> One problem that coalitions of multinational forces have yet to solve, however, is what the United States calls "sensitive compartmented information" (SCI). This is information which comes from sources . . . details of which one country does not want to share with its allies for fear of systems or sources compromise.
>
> [I]t does remain true that intelligence of some kinds continues to be a "national responsibility," thwarting the unity of multinational effort.[4]

2.7 SUMMARY

In this chapter, we have reviewed some of the roles, players, and factors that affect the marriage of intelligence collection and military operations. The discussions have certainly not been all-inclusive but they do raise other areas for discussion. In the next chapter, we will examine the Army's AirLand Battle doctrine and some of the policy implications deriving from it, review the Navy's Maritime Strategy and its C^3I policy requirements, and discuss some views of C^3I from various positions within our government. Finally, we will review some concerns of NATO with respect to C^3I policy.

CHAPTER THREE

DOCTRINE, STRATEGY, AND C^3I

To be effective, the commander must know the battlefield. He must surprise the enemy and catch him at a disadvantage as often as possible. He must avoid the enemy's strength and exploit his weaknesses. To do so, he must know the area of operations, the conditions, and the nature, capabilities, and activities of his enemy.[1]

In previous chapters we discussed C^3I priority, reviewed the organizations responsible for intelligence collection and military force employment, and discussed some of the institutional factors which complicate the fusion of intelligence to military command and control. We referred earlier to the impacts of current policies on military operations in a general sense.

In this chapter we will look at some other aspects of the C^3I interface. First, we will discuss the Army and the Air Force's AirLand Battle doctrine and some of the demands it places on C^3I. Then we will review the Maritime Strategy of the Navy and with it some ideas on the need for optimum C^3I cohesiveness. In looking at these employment principles, some questions come to mind. For example, is military doctrine and strategy supportable through the current policy structure? Is the proper emphasis being placed on the "tactical" segment of C^3I? What are the views of C^3I from Congress and the intelligence community? What are the concerns related to C^3I in multinational scenarios? We'll consider NATO as an example. Finally, what additional inferences that could impede C^3I integration can be drawn from considering the above questions? We will address these questions as we move forward in this study.

NOTES

1. John Patrick Quirk, *The Central Intelligence Agency: A Photographic History*, Foreign Intelligence Press, 1986, p. 15.

2. Roy Godson, *Intelligence Requirements for the 1980s, Elements of Intelligence*, National Strategy Information Center, Washington, D.C., 1983, pp. 6-8.

3. Lincoln Faurer, *Seminar on Command, Control, Communications, and Intelligence, Spring 1985* (Cambridge, Mass.: Program on Information Resources Policy, Harvard Univ., 1986), p. 21.

4. Lt. Gen. John H. Cushman, *Command and Control of Theatre Forces: Adequacy* (Washington, D.C.: AFCEA Press, 1985), pp. 2-31 and 2-32.

3.1 THE ARMY, AIR FORCE, AND THE AIRLAND BATTLE

Within the U.S. military services, it is generally accepted that the Army is the branch that is most entrenched in the doctrinal concept of war. It is through their doctrine that field commanders are told, in general terms, how they will employ their assigned forces. Doctrine also provides the basic framework for their concepts of operation. Today's doctrine has evolved based upon the realities of force structures, political considerations, and improved lethality of weapons.

The Army's current doctrine (which was developed in coordination with the Air Force) is called AirLand Battle. As the name implies, this doctrine emphasizes combined operations employing both air power and ground-based forces in coordinated activity. In the European scenario, AirLand Battle is the U.S. Army's doctrine, which is blended with the North Atlantic Treaty Organization (NATO) doctrine of Follow-On Forces Attack (FOFA). With the speed, range, and lethality of today's weapons, these doctrinal concepts place heavy demands upon both the intelligence and operational command and control assets of theatre commanders. Has the capability of these assets kept pace with doctrine? Is national policy "in sync" with employment demands? Let's begin by looking at the doctrine itself as a first step in considering these questions.

3.1.1 What Is the AirLand Battle?

The AirLand Battle is the Army's basic "how to fight" doctrine. It is outlined in U.S. Army Field Manual 100-5, *Operations*.[2] The doctrinal concept of the AirLand Battle is the latest of an evolving series of operational conceptual thoughts. The earlier version (1976) of the Army's doctrine, called the "active defense," had been criticized as too passive and too dependent upon maintaining defensive positions by committing virtually all assigned forces to the repelling of attacks, while holding little hope for launching counteroffensive strikes.[3] The lack of potential for being able to convert to the "offensive" did little for the military planner's optimism of eventual victory, to say nothing of an ally's desire to hold his homeland territory.

With the publishing of the 1982 version of FM 100-5, the Army moved into an era of doctrine that stresses the offense to a much greater degree. The doctrine outlines other significant changes in operational thinking. Among these are considerations that affect the requirements for both the elements of C^3 and I and their integration into the field commanders' arsenal. Speed of movement, the tendency toward counterattack or enveloping maneuver, airborne operations, and combined arms operations all tend to place increased stress on the "marriage" of the operations and intelligence functions of C^3I. AirLand Battle doctrine tends to exacerbate the need to enhance the use of tactical intelligence generated either from within the theatre assets or through expanded use of "national" assets.

Another key aspect of AirLand Battle doctrine is the introduction of the concept of the "operational level of war."[4] This term refers to the use of "military resources to attain strategic goals within a theatre of war." In previous expressions of doctrine, the Army had experienced difficulty in dealing with the doctrine for expanded employment of forces of large proportion (echelons above Corps level but short of operations of a strategic nature). Note that the basic idea of "operational level doctrine" is not really "new" to Army thinking. Many cases, from World War II experience, called for the maneuver of "Army-size" units in multiservice and multinational scenarios. More recent experience in Viet Nam, however, accentuated Army doctrinal attention on smaller unit actions.

The concept of the operational level of war was created to bridge the gap between doctrine of strategic (involving a total national level effort) and tactical (actions involving units of "smaller" size).[5] The separation of "operational" and "tactical" doctrine is not clear. "At corps and division, operational and tactical levels are not clearly separable. They are guided by the same principles."[6] The separation between the two seems to be in the dimension of the action under consideration:

> An operation designed to defeat an enemy force in an extended area does so through *operational* maneuver and a series of *tactical* actions.[7]

The discussion of C^3I support for the AirLand Battle in this chapter deals to a large extent with the dilemma of dealing with the requirements to support the operational level of war. C^3I at this level is complicated on the operational side by the multiservice and multinational environment of potential future wars. Intelligence support is made more complex by the "depth" of interest of the "operational" level commander, the bureaucratic turf boundary questions which could crop up, and the scarcity of intelligence resources which might be available to the operational commander from national assets throughout the world.

3.1.2 Has C^3I Kept Pace with the AirLand Battle?

Perhaps one of the most central questions with respect to command and control and the operational support provided to it by intelligence is has C^3I kept pace with the doctrine that has now evolved, AirLand Battle? As we discussed previously, the AirLand Battle represents a significant departure from the Army's earlier doctrinal concepts. With the combined arms action, dependence on maneuver and, most significantly, the "deep look" nature of the AirLand Battle, the need to see well beyond the Forward Edge of the Battle Area (FEBA) has changed the requirements for integrating the assets of the intelligence into the maneuver element of ground forces.

3.1.3 What Are Some of the Army's Concerns with C^3I?

Concerns have been expressed from both within and outside of the Army with the demands created by the AirLand Battle doctrine. These are related to everything from understanding the doctrine's reference to the "operational" level of war to the demands that the doctrine places on intelligence and command and control at various organizational levels of the Army. The situation of the AirLand Battle has been compared to that of a soccer game:

> Air/land battle has tremendous requirements (for C^3I) because you need CD (controlled dissemination), you need to synchronize. To give you an analogy, in air/land battle you are no longer in a football game of opposing forces across from each other, but more like a soccer game where you're entwined, and there is a lot more mobility on the battlefield. The essence of the air/land battle is flexibility and synchronization, and that requires an awful lot of command and control support systems.[8]

One of the most basic of the Army's difficulties with understanding and accepting the AirLand Battle doctrine deals with their traditional orientation toward the "tactical" level of war. For example, nearly all of the Army's training and its field manuals ("below 100-5") are oriented toward tactical thinking. Since these manuals serve as the basis for the Army's field training, no comprehensive system exists for teaching the "operational" orientation of the AirLand Battle and the command, control, and communications demands which result.[9]

The above concern has also required a change in thinking for the Army's intelligence staff elements. Their change in orientation relates to the scale of the area of interest created by the doctrine. FM 100-5 outlines the commander's "Area of Interest"[10] in Table 3-1:

Table 3-1

Commander's Area of Interest

Level of Command Objective	Time Beyond Current Attack
Battalion	up to 12 hours
Brigade	up to 24 hours
Division	up to 72 hours
Corps	up to 96 hours
EAC (Echelon Above Corps)	beyond 96 hours[11]

The time demands created by the doctrine result in intelligence "planning considerations . . . [which] require incorporation of political, psychological, . . . and geographical factors on a grand scale."[12] Operational level intelligence requirements span the "traditional" Army categories of tactical and strategic intelligence. The operational level of war addressed in the doctrine of the AirLand Battle is intended to address a level of command that had not been addressed well in earlier doctrine. Here again, the Army's doctrinal experience of World War II has not been relied upon to any great extent since the early 1970s.

Operational level intelligence is directed at the echelons of command above corps level and below the levels associated with strategic operations. More precise definitions of the goals of "operational" level intelligence are still being developed:

> It is not enough to state that the intelligence requirements of the operational-level commander will be satisfied by a fusion of tactical and strategic intelligence. The assets of the strategic intelligence community are over-extended in peacetime. They will certainly be overwhelmed during war if the goals of strategic and operational decision making are not defined.[13]

There is also concern within the Army that their intelligence elements have not kept pace with doctrine from a structure or systems perspective. The opinion has been expressed that capability of division-level intelligence assets are outfitted and organized based upon outdated "Active Defense" scenario thinking:

> But, translated into the scope,scale and fluidity of the AirLand Battle environment, we (the Army intelligence organizations) remain structured to support local tactical engagements along a nonporous FEBA.[14]

The bottom line of the current situation is that the Army's decision to move to an AirLand Battle doctrine places greater demand on both command and control and intelligence systems and organizations.

Continued interest and emphasis from leadership at all levels are needed to optimize the effectiveness of the doctrine.

3.2 THE NAVY AND THE MARITIME STRATEGY

The Army is oriented heavily in thinking of the *execution* of military operations through doctrine. Strategy level of thought within the Army has not received the same level of attention. It has been said that the Army "doesn't do strategy."[15] "Its lack of control of terrain, engagement, and supporting resources"[16] denies the Army "the freedom to define war on its own terms."[17] The Navy, on the other hand, has traditionally been much more comfortable in dealing with addressing higher level strategy goals.

In basically the same time frame as the evolution of the AirLand Battle doctrine, the Navy developed its strategy of how it would carry out national strategy objectives. The Navy's view is more global in its nature, more general in its approach, and covers a wider range of situations calling for military force to be employed.

3.2.1 What Is the Maritime Strategy?

The Maritime Strategy is the maritime component of the U.S. National Maritime Strategy. It has been written that the strategy emerged from the goal of Secretary of the Navy John Lehman's dream of "rebuilding the U.S. fleet to 600 ships from its post-Vietnam nadir of 475."[18] Included in the strategy's force structure were plans for growth to 15 carrier task forces, reactivation of mothballed battleships, and an increase in the size of naval aviation.[19]

The strategy itself addresses the use of naval military power through a range of "levels of violence" ranging from Peacetime Presence through Crisis Response to Global Conventional War.[20]

3.2.2 How Important Is C^3I?

In the warfighting level, the Maritime Strategy is described as potentially moving through three "phases." The first of these is the *Deterrence or Transition to War Phase*:

> Keys to success of both the initial phase and the strategy as a whole are the speed and decisiveness in national decision making. The United States must be in a position to deter the Soviets' "battle of the first salvo" or deal with that if it comes. Even though a substantial portion of the fleet is forward deployed in peacetime, prompt decisions are needed to permit rapid deployment of additional forces in crisis.[21]

The need for timely, accurate intelligence and sound command and control is also required for the phases of the strategy that follow. In the second phase, *Seizing the Initiative*, the need for timely, coordinated action is spelled out:

> It will be necessary to conduct forward operations with attack submarines, as well as establish barriers at key choke points . . . to prevent leakage of enemy force into the open ocean where Western Alliance resupply lines can be threatened.[22]

C^3I is also a prime cornerstone of the Maritime Strategy in its third phase, *Carrying the Fight to the Enemy*, of warfighting execution:

> Command, control, communications, and intelligence combine to form the glue that binds this entire effort together.[23]

3.2.3 What Is Key to Maritime Strategy's Success?

The Maritime Strategy's basic outline sheds much light on what it might take to give the strategy a chance at success. C^3I can be the critical key ingredient. This view has been shared by former "field" commanders as well:

> Changes in the technology of communications and of surveillance sensors today have more effect on the outcome of battles than do weapons.[24]

How well tied are the surveillance and command and control assets for the naval commander? Probably not well enough to ever satisfy most. Some things could be improved. Among these is an enhancement of the tie between the national intelligence assets and the deployed commanders. Some enhancement of understanding and communication could occur on both operational and intelligence ends of the pipeline. VADM Richardson outlines one such example, signals intelligence:

> There was then, and still is today, great reluctance to acquiesce in any shift in combat management responsibility away from the on-scene commander. However, most information giving a "heads-up" of an impending attack comes by way of Washington. It may, or may not, reach on-scene commanders in time. Consolidating signals exploitation in the Washington area was necessary for many good reasons. There was also a price to pay. We created a generation of navy flag officers with little-to-no understanding of the benefits to be had from exploiting special intelligence. We created analytical centers that were without knowledge of our own operational activity, hence with little appreciation of who needed the information they held, and in what time frame.[25]

* * * * *

> Whatever the changes in Command and Control of military forces viewed "from the top down" in Washington in legal mandates, there are immutable requirements seen "from the bottom up" that have to be met . . . to be able to target our long-range weapons. Much if not most of the operational capability and pertinent information . . . resides in Washington-area functional agencies. . . . Bridging the gap between "national level" sensor systems exploiters and deployed naval task force commanders requires extensive [coordination] that cannot be accommodated afloat. The Fleet CINCs are best suited to perform these functions.[26]

In both the AirLand Battle and the Maritime Strategy, the need for "deep-look" intelligence capability has been called for. As we discussed in chapter 2, policy, resource, and classification factors can impede the full integration of intelligence into military operations. How well are these problems understood in other segments of government?

What are the concerns of Congress with respect to C^3I? What are the views of the military application of intelligence from within the intelligence community? In the next few pages, we'll discuss these questions.

3.3 HOW IS C^3I VIEWED AT DIFFERENT LEVELS OF GOVERNMENT?

The view of the effectiveness of our C^3I capabilities depends in great measure upon the position of the person reviewing the situation. In the discussion that follows we will review concerns of two significantly different levels of government -- Congress and the National Intelligence Community. Each has its own set of concerns relating to some facet of the command, control, communications, and intelligence taskings and capabilities.

3.3.1 Perspective from Congress

Congress's view of operational command and control and intelligence capabilities and priorities often differs from various levels of the executive branch. Since the mid-1970s with the Church Commission and post-Watergate investigations, Congressional concerns have centered on two primary sets of issues dealing principally with the intelligence area. One has been the question of the legitimacy of U.S. intelligence activities in this country and in many other areas of the world. The second has centered on the moral question of the involvement of intelligence in various covert activities. The basic issue centers on the role of intelligence in a free society such as found in this country. It has been questioned many times over whether many of the tasks undertaken by the intelligence community could have been handled in other ways (or whether they should have been attempted at all). The common thread which binds these issues is the question of maintaining the proper balance of power between the law-making responsibilities of Congress on the one hand, and law enforcement taskings of the Executive branch on the other. It should also be noted here that Congressional concerns with intelligence have centered largely with *covert operations*. Much less debate has been generated relating to other intelligence

"roles" such as *collection* or *analysis and estimates*. These have been generally accepted in Congress (and elsewhere in government) as necessary and important activities required to support national security objectives.

3.3.2 The Question of Control

One of the prime concerns from Congress has centered on the degree of control retained within the Executive Branch for many of these operations. Congress seems to be doing more to "assert a claim of equal partnership with the executive on intelligence policy, organization, and operations."[27]

The expansion of Congressional involvement in intelligence questions has taken form through the Hughes-Ryan amendment as well as other actions such as the subsequent creation of the Senate and House Intelligence Oversight Committees (with their budget approval authority). All of these have served to change the traditional role of Congress into one of being "an equal partner with the executive in intelligence policy and operations."[28]

Since the Iran-Contra affair, Congressional involvement has continued, and will likely expand. One bill being considered now establishes the requirement for the president to provide Congress with a specific "finding" to authorize any covert intelligence activities within a specific time limit. The responsibility for informing Congress under this proposed legislation would be shifted from the director of Central Intelligence to the president.[29]

A second proposal also being considered involves a restructuring of the intelligence community leadership structure. Under this bill, a "director of national intelligence" position would be created, "analogous to the national-security advisor." The CIA director's responsibilities would be limited to running the activities of his agency, similar to the role of the FBI director. Creation of this new position would serve to separate the function of intelligence collection and analysis and the formulation of policy.[30]

3.3.3 The Question of "Tactical C^3I"

It may seem that most discussion within Congress with respect to the role and relative importance of intelligence has indeed centered on the "moral" aspects of the subject. It is certainly true that a great deal of attention has gone to the role and use of intelligence by our government. More specific questions involving C^3I have also been addressed with respect to the military application of intelligence. As with other military capabilities (and categories of programs which help to create the capability), the question of C^3I capability for the military comes up often when budget battles and associated tradeoffs heat up each year. In this regard, it seems that tactical command and control and associated intelligence programs have not received the same level of support as strategic programs.[31]

Several reasons for this lack of support have been outlined. C^3I's expense, complexity, lack of coordinated advocacy as well as the classification of many C^3I programs have all been cited as reasons for "cutting" these types of programs in the past.[32]

While funding difficulties may continue, the need for continued attention to tactical C^3I seems to be understood from a capability perspective, particularly as the capability applies to the NATO environment:

> The United States also should focus attention on those capabilities that will enable U.S. forces in NATO to attack Soviet follow-on forces. These deep attack systems include surveillance arrays that provide the capability to look deep into the enemy's rear areas to locate, identify and track Soviet follow-on echelons, and deep attack weapons systems, both surface and air-delivered, which are capable of striking and destroying enemy formations before they reach the main battle area.[33]

3.3.4 View from the National Intelligence Community

With Congressional views largely focused on legal, moral, or budgetary concerns, we are going to find that the intelligence community (not surprisingly) has a different perspective of the C^3 and I marriage.

C^3I integration is observed more from an operational perspective by the intelligence community. Recognition of military operational requirements is one thing, results are another.

While the problems of integrating intelligence into military command and control seem to be understood, there seem few easy-to-implement answers to what can be done to enhance the situation. The integration of national intelligence capability into the military command structure, particularly at the "operational" or "tactical" level, is extremely difficult. All of the problems mentioned in the previous chapter come into play. Policy, classification, and resource questions all complicate this integration. At the same time, all of this goes on in a "system" made up of bureaucracies the size and complexity of the Central Intelligence Agency, the National Security Agency, the Defense Intelligence Agency, the Unified and Specified Commands, and the services themselves.

Let's consider an example. As discussed in chapter 2, the National Security Agency is the "sole-source" agency responsible for collecting signals intelligence (SIGINT) for the government. The director of the NSA takes taskings from two primary sources. The director of Central Intelligence sets the NSA's general priorities. At the same time, the secretary of defense and military commanders set standards of timeliness for hostilities-related taskings.[34] The dilemma of supporting a multiple set of priorities raises difficult questions of resource control. Let's review one of the comments cited in chapter 2.

> Let me talk for a moment about SIGINT support to the military commander. A conflict exists between the desire of that commander to control his own assets, and maximum SIGINT support. Every commander will tell you he feels far more confident going into battle with control over both what will fight and what will support him. On the other hand, he currently does not have, and is unlikely to acquire (because of cost limitations) the intelligence wherewithal to fight the battle alone. The assets just can't be made available.[35]

An important fact of life within the intelligence community is the separation of intelligence responsibilities outlined in the organizational review in chapter 2. This separation occurs in part because of the individual creation and development of each agency. Once created, the agencies became self-sustaining institutions. The community is also "fragmented" because of the complexity of the systems which have evolved for supporting intelligence taskings. This "splitting" of organizational taskings contributes to difficulty in supporting military operations:

> The intelligence community is institutionally fragmented. It is spread out through several executive departments. Its biggest customer is the military. For that reason, it is intertwined with the military services. Getting this fragmented community to operate effectively with the military is not easy. When it does act as a whole, and when it does accept its intimate relationship with the operational staffs of the services and the unified commands, the results are truly impressive. Making progress in this regard brings turf conflicts, concerns with security, concerns with who gets the credit. Sometimes, ignorance of our capabilities, both within the Intelligence Community and within the services, causes a less than desired result. New technologies, delicate operational details, and lack of experience in coordination also add to the difficulties in achieving all that is possible in providing intelligence support. We should not be surprised, therefore, at some of our failures, but we also should not be parochial in overcoming them. The symbiosis that we gain through cooperation is remarkable, too remarkable to let cooperation go unattended. The trend in this regard is good, but there is a long way to go.[36]

The marriage of C^3I functions for U.S. military employment purposes has demands placed on it by the military's doctrine and strategy, may not be fully understood in some segments of Congress, and is complicated by the institutional fragmentation of government bureaucracy. There are still other factors that can influence C^3 and I integration, particularly in the multinational environment. In the following section, we will highlight some of these factors -- including force

balance, strategy, Allied commitment, and systems development concerns -- by looking at NATO and some concerns related to C^3 and I in that alliance.

3.4 WHAT IS THE NATO PERSPECTIVE?

When the situation in NATO on any defense related topic is assessed, the impact that the recent arms control developments between the U.S./ NATO and the Soviet Union/Warsaw Pact might have on the subject must be considered. Even if the INF Treaty is ratified and the weapons covered by the agreement are taken out of commission, the essential balance of forces in the European theatre will remain a subject of great concern on both sides of the Atlantic.

In the discussion that follows, we will consider several areas that relate to doctrine, strategy, and C^3I in the NATO arena. First, we will briefly review the conventional force balance that exists between NATO and the Warsaw Pact. Then, we will review some recent sources in an attempt to sense potential shifts in Soviet strategy and doctrine that might, in turn, lead to a change in NATO doctrinal stance. Finally, we will consider C^3I capabilities in the European theatre in order to enhance our understanding of improvements that are needed or being worked.

3.4.1 Force Balance

The conventional force balance in Europe remains a source of prime concern to the NATO alliance. The numbers alone are staggering. In Central Europe, the Soviets possess numerical superiority in tanks (18,000 to 12,700), artillery (9,500 to 3,600) and fighter aircraft (1,020 to 304).[37] When all forces from the Atlantic to the Urals are considered, the numbers are even more sobering. The Warsaw Pact holds an advantage of 52,200 to 22,200 in tanks, 37,000 to 11,100 in artillery, and 4,930 to 899 in fighter aircraft over NATO forces.[38] The balance of these forces has been the subject of debate for some time. With the apparent desire of current Soviet leadership for arms reduction

talks to go beyond the INF limitations, the subject is a hot item in NATO circles. "The paramount interest now (within NATO) and the only game in town is conventional weapons and the talks with the Soviets," observed Thomas Kielinger, editor of the newspaper *Rheinischer Merkur*.[39] If conventional arms reduction talks lead to any significant shift in the force ratios outlined above, shifts in doctrine are likely to eventually occur as well. There has been some indication on the part of Soviet leadership that there may be some willingness to negotiate in this direction. "We are prepared to reduce the arms in which we have an advantage," Gorbachev stated in Moscow on 11 January 1988.[40]

Countering the optimism of the above are reports of the continued efforts on the part of the Soviets to upgrade their military hardware. Reports in January 1988 indicate that the Soviets are developing an improved main battle tank contributing to a narrowing of the "technology gap." The "qualitative" edge of NATO weapons systems has long been the redeeming quality of arms comparison discussions in Europe.

3.4.2 Strategy Shifts?

With the INF agreement, speculation has emerged that there might be some shift by either the Soviets or NATO in their theatre strategies.

On the Soviet side, it has been reported that under Gorbachev, Soviet doctrine has ceased to be "offensive" and is now "defensive." The phrase now being used by Soviet spokesmen is that of "non-offensive defense." Other reports claim that this latest play on words has no meaning at all. They believe that Soviet war-fighting principles will continue to be based upon the same four principles as those of the pre-Gorbachev era: offensive strikes on the eve of hostilities, surprise and concealment of the preparations for such strikes, denying enemies the ability to choose their timing and manner of attack, and maintenance of military superiority over any possible enemies, both in quality and quantity.[41]

On the part of NATO, concern has been voiced that speculation such as that outlined above might lead to shifts in the NATO counter-strategy,

or even a serious split in the structural integrity of the alliance itself. However, March 1988 reports from NATO indicate that such a split is not likely to occur. Leaders expressed continued concern with the conventional arms balance in Europe and advocated the continued need for a strategy of "flexible response" based upon both conventional and nuclear weapons.[42] This position was also voiced by the NATO commander in a separate interview. The strategy of forward defense and flexible response continues to be this commander's marching orders.[43] General Galvin did recognize the concern of some West German groups with the continuation of NATO's need for nuclear weapons:

> I don't know if I could ever answer German worries about "singularization." NATO's theater nuclear weapons are the main deterrent to war.[44]

Maintaining the solidity of the NATO alliance in spite of Soviet initiatives will continue to present a formidable challenge to future leadership, both in the U.S. and throughout NATO.

3.4.3 C^3I in Europe

Whether the underlying strategies of NATO and the Warsaw Pact change significantly in the foreseeable future remains to be seen. Regardless, there remain some essential challenges to the effective employment of NATO's forces in the European theatre.

The C^3I links of NATO are at the core of the alliance's chances of succeeding in any armed conflict scenario against the numerically superior forces of the Warsaw Pact. The need for an effective link of intelligence and operations in force employment has never been needed more than in the European scenario. From a doctrinal perspective, NATO's Follow-On Forces to Attack (FOFA) is consistent with the U.S. Army's AirLand Battle. It is offensive in its orientation and for that reason places a significant reliance upon intelligence and its link to operations.

3.4.4 Allied Commitment to Intelligence

As with the emergence of U.S. intelligence agencies, the commitment of NATO members toward intelligence has its foundation in the remnants of World War II. For example, the ties between U.S. intelligence agencies and those of the United Kingdom can be traced to the war and have been well-documented.[45]

The commitment of another NATO ally is also related to the war experience, but in a different way. West Germany's commitment to intelligence as a discipline is complicated by the war experience. Although West Germany recognizes the proximity and threat posed by the Soviets and the Warsaw Pact, it does not look upon intelligence in the same way:

> [I]ntelligence does not appear to have the same influence or institutional status as it does in Washington. The West German Chancellor does not have a National Security Advisor or an intelligence staff of his own. While secret intelligence is undoubtedly factored into West German decision making, the West German intelligence chiefs stay well clear from any appearance of influencing policy. . . .[46]

West Germany does seem to understand the importance of intelligence in contributing to their national security and appears ready to support intelligence for military application:

> As long as the intelligence efforts are perceived as contributing toward those [meaning military] objectives, the West Germans will happily shoulder the costs of their federal intelligence services.[47]

Although the main thrust of this paper is to study policies that impact the marriage of operations and intelligence in C^3I, a brief look at some related systems helps put the importance of the subject as well as the views of various players into perspective.

3.4.5 Systems Development

If one assumes that the philosophical questions of shifting strategies and national commitment within NATO are satisfied, concern may then center on the question of actual capability. One measure of capability (and the concern over the lack of it) is to take a look at systems under development to improve the capability. From the standpoint of C^3I systems development, there appears to be an awareness of the need for some enhancement within NATO. The degree of actual commitment to particular systems and programs varies. This seems to be particularly true with respect to the fielding of surveillance and intelligence support systems. Let's review some of the more significant of these systems now being developed.

3.4.5.1 Stand-off radar systems

Several programs are being worked independently by the U.S., United Kingdom, and France to develop an enhanced capability to detect and track both stationary and moving ground targets some distance behind the Forward Edge of the Battle Area (FEBA). These systems would be valuable in detecting and attacking tanks, armored vehicles, trucks, and other vehicle concentrations of the enemy theoretically before they could be brought into play and influence battlefield actions at the front lines. These systems are being designed to offset a shortfall in NATO's surveillance capability:

> NATO's current systems and procedures probably are capable of supporting the attack of targets that do no move frequently, but they fall far short of providing broad, deep, continuous coverage and targeting data on highly mobile systems, especially those that do not emit radar or radio signals. At present, only fixed targets and vehicles that halt for relatively long periods can be acquired reliably.[48]

One of the systems now being developed is called the Joint Surveillance Target Attack Radar System (Joint STARS). This system is projected to serve an air-to-ground role in a manner similar to the air-to-air role performed by the Airborne Warning and Control Systems (AWACS). Joint STARS is being designed "to detect and indicate moving

ground vehicles and to guide attacking aircraft and missiles to moving or halted formations of enemy vehicles."[49] The system itself consists of an E-8A (Boeing 707-type) airframe and one or more ground station modules (GSM). The aircraft are being equipped with side-looking radar (3cm-band designed by Norden)[50] and several links to advanced communications systems. Radar data from the aircraft will be transmitted by data link to the ground modules. Control and operation (projected to be done jointly by the Army and Air Force) of the radar could be conducted from either the aircraft or ground modules.[51] The Joint STARS program is widely supported within the defense community of the U.S. and NATO. The program has been contested in Congress based upon arguments primarily centered around its utility and vulnerability to attack.[52] The Joint STARS production decision (program cost is about $4 billion) is projected for October 1990.[53]

3.4.5.2 Unmanned aerial vehicles

Another surveillance system category that has received attention is unmanned aerial vehicles. These have been considered as a possible way to accomplish the reconnaissance of more limited areas without jeopardizing a manned aircraft. Programs to develop such systems have been undertaken by the U.S., Israel, Italy, Canada, and the U.K.[54] The U.S. system, developed by the Army and using the Aquila drone, is called the Target Acquisition Designation Aerial Reconnaissance System (TADARS). This system has been envisioned to function as a surveillance and target designation system to perform target acquisition, artillery fire adjustment, and laser guided weapons guidance as well as damage assessment roles.[55] However, performance problems have led to the cancellation of this $2 billion program by the Army in an FY89 budget decision.[56] Success with other types of unmanned air vehicles has been noted by the U.S. The Navy, in recent operations in the Persian Gulf, has been pleased with the operation of Israeli designed "Pioneer" remotely piloted vehicles, which they used for surveillance purposes from the battleship *Iowa*.[57]

3.4.5.3 Other surveillance systems

Still other surveillance systems are under development by the U.S.'s NATO allies. The French, for example, are developing their own version of the Joint STARS concept. This system, called Orchidee, uses the Mk 2 Super Puma helicopter to carry aloft a radar capable of "seeing" 150 km. The radar data are relayed to one of two ground stations for processing and operational "use." This system is augmented with the employment of reconnaissance drones for use by corps commanders who want to explore in greater detail specific areas originally uncovered by an Orchidee detection. Flight tests of the Orchidee system will last until early 1989.[58]

A German system, which would use the same radar used in early tests of the French Orchidee system, uses an unmanned Dornier Priamos helicopter hovering 10,000 feet above the battlefield and carrying a shorter range surveillance radar to cover sectors 40 to 50 km behind enemy lines.[59]

The British are in the process of developing two systems for enhancing battlefield surveillance. The Airborne Stand-off Radar (ASTOR) program is very similar to the French Orchidee. The U.S. and U.K. are working jointly to develop this system, which would be linked to the Joint STARS ground stations.[60]

The second British system is a side-looking aperture radar carried in a Canberra aircraft flying at an altitude of 60,000 feet. This system is projected to cover roughly the same area as the Joint STARS (up to 200 km behind enemy lines), with its data sent to ground stations for relay to the Army Corps.

If the systems discussed here are eventually fielded, operational commanders in Europe will possess the capability to obtain a much improved picture of enemy formations than is now available and under their control.

3.4.6 Information Explosion

At risk with the enhancement of systems developed to provide commanders with the data they need to fight the war is an associated danger that there will be more information available than can be absorbed and used:

> With rapid technological advances and the proliferation of sensors, however, we risk drowning in data rather than being supplied with information. Intelligence fusion supported by automated data processing capable of distilling the volumes of raw data becomes vital. Equally important is the dissemination of the right information to the appropriate level of command. Minute detail does not help the commander if it gets in the way of the decision making process.[61]

The complexity of the problems outlined above is formidable, if not impossible. However, the situation is being addressed.

3.4.7 Battlefield Information Collection and Exploitation System

The Battlefield Information Collection and Exploitation System (BICES) is a program of programs "which seek to address the question of timely intelligence support, fusion and dissemination in NATO."[62] The goal of BICES is to provide "a complete picture of the battlefield, portraying both friendly and enemy force, ground and air."[63] The need for such a system is based upon the recognition of an old problem:

> NATO consistently has struggled throughout its history with inadequate intelligence support. Intelligence always has been regarded as a national asset, covering only those areas of specific interest to the individual nations . . . . This system of intelligence collection and exploitation results in information gaps and untimely information processing that severely hinders the decision making process of the commanders. . . . Those in the intelligence field have worried about the fragmented NATO intelligence structure and the lack of an automated command control information capability to integrate the available intelligence inputs in a timely and comprehensive manner.[64]

In order to develop a set of programs, such as the ones associated with BICES, many obstacles must be overcome. Among the toughest of these is the need to develop an automated "secure gateway" for the system which will allow sanitized intelligence information to be input into the system from multiple sources.[65] When you consider the classification problems that exist within the various NATO national intelligence communities, this isn't an easy situation to overcome. BICES does offer the hope of pulling together the intelligence resources of the NATO community. Without pursuing this option, the balance of conventional forces in Europe will continue to exist overwhelmingly in favor of the Warsaw Pact.

3.5 WHAT ARE THE C^3I POLICY FACTORS?

In this chapter, we have discussed two important service doctrine and strategy schemes, reviewed some of the more prominent views from Congress and the intelligence community related to C3 and I, and looked at some prime concerns impacting C^3 and I in one important multinational defense alliance -- NATO. Similar to the discussion at the end of chapter 2, related policy factors can be drawn from the discussions of this chapter. These consist of factors related to the service's doctrine and strategy, the advocacy of C^3 and I programs, the influence of technology, and the problems of interoperability. Let's consider each of these.

3.5.1 The Doctrine and Strategy Factor

Doctrine and strategy schemes like those previously discussed in this chapter create their own set of factors related to the union of C^3 and I. First, both doctrine and strategy are developed in response to the doctrine and strategy of adversaries. As discussed earlier in the NATO section, potential shifts in Soviet strategy in Europe have raised a great deal of interest in that theatre. Why? Because changes in the Soviet's strategic "game plan" in Europe would ultimately lead to reevaluation of NATO's strategy. The NATO case is just one example.

The same logic can be applied to U.S. strategy at either the national or service component level. Soviet actions influence U.S. response, and vice versa. All of this filters to impacts on force employment shifts and C^3I conceptual changes. There are other ways doctrine and strategy impact C^3 and I.

The AirLand Battle doctrine and the Maritime Strategy were developed by the service staffs. These expressions of doctrine and strategy tell military commanders, in broad terms, "how to fight the war" in their areas of responsibility. OK, so far. But we've seen in reviewing both of these doctrine and strategy examples, C^3 and I problems can result from the creation of "new" employment concepts. The doctrine or strategy "game plans" can place demands on theatre forces for which they are not necessarily trained, may not be properly organized and equipped, or require assets (such as national intelligence assets), which lie outside the theatre CINCs' span of control. All too often the net result is that "ad hoc" C^3 and I arrangements are developed which circumvent established chains of command. Sometimes these prove to be successful (as in the case of the Persian Gulf operations), but sometimes they prove disastrous (as in the cases of the Iranian hostage rescue attempt operation and the Marine Corps barracks bombing incident in Beirut).

3.5.2 The Advocacy Factor

Another important factor that was touched upon in this chapter relates to the advocacy of C^3I programs. In chapter 1, the point was first raised relating to the value of C^3I in combating the element of surprise. In Congress, for example, this value may not be fully appreciated or understood. Congressional concerns in recent years related to intelligence haven't dealt as much with the linkage of intelligence to military operations as they have in obtaining and maintaining the proper control of intelligence activity.

A second aspect of the "advocacy factor" deals with the support of C^3 and I programs intended to enhance actual capability. Advocacy of C^3I types of programs has been difficult to pull together for several

reasons. First, it is difficult to "quantify" how many more aircraft could have been shot down, ships sunk, or tanks destroyed if "X" amount of additional C^3I assets had been available in a given employment situation. Second, C^3I systems are difficult to "visualize." Somehow looking at banks of computers or radio receivers doesn't instill the same sense of awe as "touching and feeling" an M-1 Abrams tank or an F-15 Eagle fighter. Third, many weapons systems are bought by and allocated to single-service, single-nation users. C^3I systems are often developed with the intention of being used in multiservice and/or multinational scenarios. Some of the systems mentioned earlier in this chapter fall into these categories. The more "players" who become involved in these types of procurement situations, the more difficult it is to obtain consolidated advocacy. Why? Because one "player" believes he is having to sacrifice more in another mission area to pay his share of the system's cost than his co-developer, or that he is gaining less with his portion of the program's cost.

3.5.3 The Technology Factor

Another factor that can impact C^3I capability is related to technology. In the NATO section of this chapter, we reviewed several programs being developed with the intent of enhancing NATO C^3 and I surveillance capabilities. In addition to the concerns with advocacy outlined earlier, technology can affect whether these programs are actually procured. Sometime in the development process, decisions must always be made on whether the technology investment being considered is worth the risk, operational utility, and cost of the program.

3.5.4 The Interoperability Factor

Interoperability also impacts the C^3I "marriage." The ultimate "link" of command and control and intelligence system interfaces is communications. The difficulty of linking these complex systems is especially tough in multinational, multiservice situations. To be successful, interoperability must go beyond technical interface questions.

Interoperability has to be considered in functional terms. Computers must be able to interface with other computers. The interfacing must go beyond this. Interoperability also needs to consider strategy, doctrine, and systems -- all of the components of force employment in order to achieve truly functional C^3I interoperability.[66] Put another way, the concept of interoperability needs to be remembered as "the interoperability of command and control *systems* -- people, doctrine, and procedures as well as equipment."[67]

3.6 SUMMARY

In this chapter, a variety of topics have been addressed that relate to the importance of a close "marriage" of intelligence to military operations. We began this review by looking at the Army (and Air Force) AirLand Battle doctrine.

The AirLand Battle is a doctrine that stresses momentum and taking to the offense at the earliest opportunity. In order for it to be effective, information about the strength and disposition of hostile forces must be known to friendly commanders early. The theatre commander's area of interest, for example, extends more than 96 hours ahead in time. With the speed of maneuver of modern-equipped armies, intelligence capabilities of friendly forces may require the dedication of national-level assets.

Next, the Navy's Maritime Strategy was reviewed. Although it is more global in perspective than the doctrine of the Army, some similarities exist between the two. The Maritime Strategy is one of forward defense. It also calls for seizing the initiative and moving to the offense early on. For this reason, the strategy also requires the integration of national intelligence assets into the operational commander's "arsenal."

In this chapter, the views of some senior leadership from both Congress and the national intelligence community were also considered. While much of the discussion within Congress relating to intelligence

activities has centered on legal and moral issues, it is not apparent that there is a fundamental understanding of the problems of C^3I within the leadership of some segments of Congress.

Within the intelligence community, it seems that the theatre commander's requirements for intelligence are understood. The problem from this level is centered on the question of priority. While the intelligence community may understand military operational requirement, the resources to support them may not exist, particularly when matched against competing priorities.

The next section of this chapter focused on NATO and some of the unique problems that Europe presents to the C^3I marriage. From a strategy and doctrine perspective, things remain relatively stable in Europe in spite of the recent INF Treaty.

The requirements for C^3I, therefore, are tied to NATO's Follow-On Forces Attack (FOFA) doctrine (and the U.S. Army's AirLand Battle part of that). Based upon doctrine, there is a need for an effective means of dealing with the Warsaw Pact's continuing numerical superiority in conventional weapons. One solution is to develop systems that possess the ability to "see deep" into Eastern Europe. When needed, these systems could then direct NATO air power against hostile force concentrations before they could influence the potential war's outcome. A number of systems are being developed within NATO to enhance this capability, some of which were reviewed in this chapter.

The review of these systems led back to a point of earlier discussions. Without the proper integration of information, the field commander may find himself with another concern. Rather than suffering from "information starvation," commanders of the future may find themselves with more information available than they can handle. Future policy decisions must address this situation as well.

Finally, a number of factors affecting the C^3 and I interface drawn from the discussion topics of this chapter were also reviewed. These include factors related to doctrine and strategy, advocacy of programs, technology, and interoperability. Each of these can influence C^3 and I capability and must be considered in future policy development.

NOTES

1. Field Manual 100-5, *Operations*, Headquarters Department of the Army, Washington, D.C., 20 August 1982, p. 6-1 (hereafter, Field Manual 100-5, *Operations*).

2. Ibid.

3. John H. Maurer and Gordon H. McCormick, "Surprise Attack and Conventional Defense in Europe," *Orbis-A Journal of World Affairs* 27, no. 1 (Spring 1983): 116-117.

4. Field Manual 100-5, *Operations*, p. 2-3.

5. Ibid.

6. Ibid.

7. Ibid.

8. Lt. Gen. Clarence E. McKnight, Jr., "C^3I Systems at the Joint Level," *Seminar on Command, Control, Communications, and Intelligence, Spring 1986* (Cambridge, Mass.: Program on Information Resources Policy, Harvard Univ., 1986), p. 24.

9. John E. Turlington, "Truly Learning the Operational Art," *Parameters: Journal of the U.S. Army War College* 17, no. 1 (Spring 1987): 61.

10. The commanders' "area of interest" includes all territory that affects their current operations (area of influence) and also extends to adjacent territory occupied by enemy force capable of affecting a commander's operations in the near future. For a complete discussion, see Field Manual 100-5, *Operations*, p. 6-2.

11. Field Manual 100-5, *Operations*, p. 6-2.

12. Capt. Larry V. Buel, "Intelligence Preparation of the Battlefield," *Military Review: The Professional Journal of the U.S. Army* 67, no. 10 (October 1987): 25.

13. Ibid.

14. Col. Leonard G. Nowak (ret.), "Division Intelligence: Left in AirLand Battle's Dust," *Military Review: The Professional Journal of the U.S. Army* 67, no. 11 (November 1987): 53.

15. Carl H. Builder, "The Army in the Strategic Planning Process: Who Shall Bell the Cat?" The Rand Corporation, April 1987, p. 14.

16. Ibid., p. 73.

17. Ibid.

18. Norman Polmar and Dr. Scott C. Truver, "The Maritime Strategy," *Air Force Magazine* 70, no. 11 (November 1987) 71.

19. Ibid.

20. Admiral James D. Watkins, "The Maritime Strategy," *Proceedings*, U.S. Naval Institute, January 1986, p. 8.

21. Ibid., p. 9.

22. Ibid., p. 11.

23. Ibid., p. 13.

24. VADM David C. Richardson (USN ret.), "Intelligence: Recollections on its Exploitation," *Wings of Gold*, Association of Naval Aviation (Winter 1987) 42.

25. Ibid., pp. 42-43.

26. Ibid., p. 45.

27. Harry H. Ransom, "The Intelligence Function and the Constitution," *Armed Forces & Society* 14, no. 1 (Fall 1987) 45.

28. Ibid., p. 50.

29. E.A. Wayne, "Tightening the Reins on US Intelligence," *Christian Science Monitor*, 13 November 1987, p. 1.

30. Ibid.

31. James P. Coyne, "The Senate and C^3I: Interview with Senator John McCain (R-Az)," *Signal* 42, no. 3 (November 1987) 27.

32. Ibid., p. 34.

33. Ibid., p. 35.

34. Lincoln Faurer, "The Role of Intelligence Within C^3I," *Seminar on Command, Control, Communications, and Intelligence: Guest Presentations, Spring 1985* (Cambridge, Mass.: Program on Information Resources Policy, Harvard Univ., 1985), p. 18.

35. Ibid., p. 21.

36. William E. Odom, "American Intelligence: Current Problems in Historical Perspective," *AFIO Periscope* (10 October 1987) 8.

37. Richard Whittle, "Conventional Forces Next Focus for Talks," *Dallas Morning News*, 11 April 1988, p. 1 (hereafter, "Conventional Forces").

38. Karen DeYoung, "Look at Arms Balance Tips with the Times," *Washington Post*, 11 November 1987, p. 30.

39. "Conventional Forces."

40. Ibid.

41. From a letter to the editor of the *New York Times*, from Joseph Churba, president, International Security Council. The letter was printed on page 26 of the 23 March 1988 edition of the *New York Times* and was written in response to an article which appeared in the 7 March 1988 edition of the *New York Times*, front page.

42. William Tuohy, "Carrington Expects NATO to Reaffirm Basic Strategy," *Los Angeles Times*, 1 March 1988, p. 7.

43. Conversation with NATO Commander General John Galvin, "The Book on Gorbachev's Design," *U.S. News and World Report* (7 March 1988) 44.

44. Ibid.

45. Among other published works, two books published in the mid-1980s contain several examples of cooperation between intelligence agencies of the United States and the United Kingdom: James Bamford's *The Puzzle Palace*, Houghton Mifflin Company, 1982, and Peter Wright's *Spycatcher*, Viking Penguin Inc., 1987.

46. Tom Polgar, "Intelligence Services of West Germany," *International Journal of Intelligence and Counterintelligence* 1, no. 4, p. 94.

47. Ibid., p. 95.

48. Michael B. Callaham, "Reconnaissance, Surveillance, and Target Acquisition for Follow-On Forces Attack," *Signal* 42, no. 2 (October 1987) 84 (hereafter, "Reconnaissance").

49. Ibid.

50. Brian Wanstall and Ramon Lopez, "Second Echelon Surveillance: Stand-off Radars to Even Battlefield Odds," *Interavia* (November 1987) 1152 (hereafter, "Second Echelon Surveillance").

51. "Reconnaissance."

52. Ibid., pp. 84-86.

53. "Second Echelon Surveillance."

54. Ibid., p. 88.

55. Ibid., p. 87.

56. Interview with Secretary of Defense Frank Carlucci, "Biting the Bullet," *Barron's* (4 April 1988) 70.

57. "US Navy Lauds Gulf RPV Success," *Flight International* (12 March 1988) 12.

58. "Second Echelon Surveillance," pp. 1154-1155.

59. Ibid., p. 1155.

60. Ibid.

61. General Leopold Chalupa (Federal Republic of Germany), "Controlling Tactical Air and Ground Forces within the Central European Command," *Signal* (October 1987) 38.

62. Ibid., p. 39.

63. Ibid.

64. VADM Jon L. Boyes (ret.), "President's Commentary," *Signal* (October 1987) 19.

65. Ibid.

66. Robert E. Mockos, *NATO Tactical Ground C^3: Interoperability Is Not Enough* (Cambridge, Mass.: Program on Information Resources Policy, Harvard Univ., 1983), pp. 38-39.

67. Lt. Gen. John H. Cushman (U.S. Army ret.), *Command and Control of Theatre Forces: Adequacy* (Washington, D.C.: AFCEA Press, 1985), p. 2-47.

CHAPTER FOUR

POLICY CONCLUSIONS

This study has centered on many factors related to the marriage of intelligence to military operations. This chapter will review some of the more important of these factors in an attempt to reinforce many important points discussed throughout this study. All of these are related to the purposes and issues outlined at the beginning of this report. We will begin by returning to some of the points initiated in the opening chapter.

4.1 PRIORITY

The subject of C^3I is an important one. From the president's statement of national security priorities through the strategy statements of the Joint Chiefs of Staff and the military services, a common thread runs with respect to C^3I. The importance of national intelligence capabilities and command, control, and communications in insuring the most effective employment of the nation's military forces are emphasized time and again.

The importance of and national commitment to these types of activities can be measured other than through policy statements. The size of the nation's "black budget" is one way of measuring such priority.

"Black budget" refers to the portion of the federal budget devoted to programs that have "restricted access" associated with them. Data concerning these programs, which include the Stealth bomber and many of the devices used for electronic surveillance, "remain hidden from the scrutiny of taxpayers, the majority of members of Congress and others who, in the Pentagon's judgment, don't have a 'need to know'."[1]

4.2 ADVOCACY DILEMMA

The size of the black budget is only one aspect related to these types of programs. Another is the question of the advocacy of these programs as they are being procured. One former commander of the Air Force's Systems Command describes the problem of C^3I advocacy in this way:

> In the broader sense, though, my experience tells me that one of the toughest aspects of C^3I advocacy is how difficult it is to quantify the benefit you will get from them [referring to C^3I capabilities], as we have to do with anything else we advocate in the Department of Defense. You can't begin to get a bomber or fighter started unless you prove its cost effectiveness down to the fifth significant figure. Not so C^3I, mainly because we don't know how to do it.[2]

The difference on what the players expect from C^3 and I programs also affects advocacy. One example is the question of tactical intelligence capability. The view of the value of tactical intelligence is different within the services themselves. The Air Force, for one, is generally concerned with the tactical intelligence capability that the pilot can "strap to his leg" and take off with. The Army, on the other hand, is much more concerned with (and supportive of) tactical intelligence capabilities.[3] This difference in view is understandable based upon the difference in the service's mission perspectives. However, such divergence of opinion doesn't help the consolidation of advocacy for individual programs when budget priorities have to be satisfied.

4.3 THE CLASSIFICATION AND CONTROL DILEMMA

In chapter 2, classification was discussed as a factor that can impede both deliberations in Congress and operations undertaken by the military. How much should be kept secret and how much should be shared? Within our government, it seems this question is continually being addressed without any apparent resolution.

In chapter 3, Congressional positions were reviewed that related to the legality and morality of some intelligence activities. The result of the many Congressional investigations that have taken place in recent years has led to the other half of dilemma -- the question of control.

Some unexpected twists have taken place that relate to the classification and control dilemma. One, which came to light in early 1988, involved the National Security Agency (NSA). The case involved NSA's refusal to release some intelligence equipment to National Guard units in two states because of concern that the equipment could be used "for the purpose of spying on political enemies."[4] The statement issued by the NSA went on to state that their concerns were with "legal policy"[5] and stemmed "from the responsibility of the director of the NSA to maintain and operate a unified intelligence activity in support of national foreign intelligence objectives."[6] Theoretically, a field commander who would gain these units in the event of a national mobilization might be surprised at the level of support his "Guard augmentees" could really provide.

A second problem associated with the classification and control dilemma is the one posed by leaks of sensitive information. There is continual finger-pointing throughout our government at who is more guilty of releasing sensitive information -- Congress or the Executive branch. Regardless of the source, there is evidence that the problem is real and the result could jeopardize military operations.

A third spin-off of the classification and control dilemma revolves around the black budget programs discussed earlier. The problem in this area is that control of information about these programs is held so tightly that the financial health of some of the companies involved can be jeopardized. One report in early 1988 told this story. The Lockheed Corporation suffered some serious financial problems in the 1970s. Before they could secure additional loans to keep their business alive, bankers had to be granted special limited clearances in order to evaluate the true "health" of Lockheed's finances. The reason: Lockheed was involved heavily in black Defense programs. The data about

these programs could not be discussed without proper clearance.[7] Is all of this control needed? At least one government official thinks the controls may be too restrictive. According to Maynard C. Anderson, the Defense Department's director of security plans and programs

> There is far too much information being classified at too high a level. Some of these special-access programs don't need to be under special access.[8]

4.4 THE TECHNOLOGY DILEMMA

The use of technology as the compensating edge against numerical superiority has been the approach taken by the U.S. and NATO in Europe for several years. In light of the INF treaty and the swing away from nuclear weapons' desirability in many parts of NATO, the tendency toward maintaining some sort of technological edge in weapons will probably continue. Pushing the edge of technology has high costs associated with it and, therefore, creates its own dilemma.

In chapter 3, we touched upon a number of systems being developed or proposed. Each of these is being developed to satisfy a specific operational need. Most of those discussed are directed at the detection of enemy formations well behind the FEBA. Consider briefly the technology dilemma associated with these and some other related programs.

The Aquila drone was one of the systems discussed earlier. This system consists of an unmanned aircraft designed to fly behind enemy lines, detect enemy formations, relay data about these targets to ground stations in friendly territory, and guide laser-guided weapons fired from friendly ground or airborne systems to destroy the target it had uncovered -- an optimistic goal that seems to have pushed the edge of technology. The system was planned to be an inexpensive way of finding enemy tanks without the risks of a piloted system. The program did not prove to be successful. In operational tests conducted in 1987, the system met all design requirements on only seven of 105 flights.[9] In

addition, development costs of the system rose from $100 million to nearly $1 billion. As a result, the system was cancelled early in 1988. The cost of the technology was simply too high.

Another system discussed in chapter 3 was the Joint STARS system. Although this program has not been cancelled, development problems with the system's radar have been experienced. Reports are that a program slip of at least one year may occur due to technical difficulties experienced by the radar's developer. The total cost of the program is $4 billion for the ten aircraft that the Army and Air Force now plan to buy.[10]

4.5 THE INTEROPERABILITY DILEMMA

Interoperability is another broadly defined dilemma that complicates the interleaving of intelligence into military operational command and control. "Interoperability . . . is the greatest single problem in theatre forces."[11] The term itself is difficult to define but, in this discussion, interoperability means that "we are speaking of . . . the interoperability of command and control *systems* -- people, doctrine, and procedures, as well as equipment."[12] Much of the discussion of chapter 3 was related to the interoperability dilemma. The consistency of doctrine, strategy, allied viewpoints and systems development are all involved. In considering theatre force employment, it all boils down to the fact that "today we have to think in the context of the *multinational air/land battle force*."[13]

There is awareness of the interoperability dilemma. In the U.S., the Goldwater-Nichols Reorganization Act of 1986 was initiated with the desire on the part of Congress to improve the interface between services as well as the interplay between the operational commands and the services. The BICES system mentioned in chapter 3 is a concept directed at improving "understanding and coordination of Allied command, control, communications and intelligence (C^3I) support and skills."[14]

Programs being developed to support C^3 and I functions must consider the interoperability factor. In NATO, this is beginning to occur:

> From a policy standpoint, the NATO C^3 system has had to evolve from a simple philosophy of trip-wire response to the elaborate requirements necessary to support the strategy of flexible response. The simplistic communications systems necessary for massive nuclear retaliation of the trip-wire era have been replaced by the need to provide a robust, interlinked C^3 system capable of selectively and flexibly responding to a conventional and/or nuclear threat in many areas and in many ways.[15]

In order to meet the above requirements, a lot of pieces to the C^3I puzzle have to be fit together. Efforts are continuing the attempt to make this happen.

Let's consider an example of one mission area. Several programs have been launched to standardize data gathered from different airborne reconnaissance systems:

> The U.S. Air Force "recently awarded two contracts valued at $500 million . . . to design a reformatter system that will allow a ground processing station to accept electro-optical data from a variety of U.S. reconnaissance sources."
>
> * * *
>
> The U.S. Air Force and Navy are currently involved in a major program to transition from film-based cameras to electro-optical systems, which can download reconnaissance imagery to ground stations in near realtime.
>
> * * *
>
> The Air Force . . . seeks to develop a common electro-optical suite that can be used on both manned and unmanned aircraft. . . . A parallel program is under way to develop a Joint Service Imaging Processing System (JSIPS) to receive and process this data.
>
> * * *

> NATO's Air Group 4, which is responsible for intelligence issues, is sponsoring a separate program to study a long term solution to standardize electro-optical data.[16]

The interoperability dilemma is not an easy one to grasp. Close attention to interoperability must be continued at every level in order for it to be an "accomplishable" goal.

4.6 THE "NATIONAL ASSET" COMMITMENT DILEMMA

Another dilemma mentioned earlier in this paper is the one related to the commitment of "national-level" intelligence assets at the tactical or operational level. In earlier discussion, several points were touched upon. One of these was directly related to policy at a national level. The president's *Executive Order 12333* excludes intelligence activities that support tactical operations from the National Foreign Intelligence Program.[17] An implication from this statement could be drawn that national-level assets for intelligence collection and dissemination are not for the use of the tactical commander. In fact, this has not been the case.

Based upon the operational doctrine outlined in earlier discussions, it seems apparent that the need for national-level intelligence will continue to increase. The fusion of information from all intelligence systems has been considered as "the future of the intelligence environment."[18] The need for improvement in the integration of this type of information at various levels in theatre C^3I networks is a challenge which requires continued *attention*.

4.7 SUMMARY

In this paper, we have discussed a number of topics related to factors that influence the integration or "marriage" of intelligence to military operations. We have certainly not covered them all. The goal has been to stimulate thought and to draw attention to the need to optimize the link between these two important functions, both of which are essential to national security. We hope that this paper will serve as a means to that end.

NOTES

1. Kathryn Jones, "Mystery Shrouds Contracts," *Dallas Morning News*, 6 March 1988, p. 1.

2. General Robert T. Marsh (USAF ret.), "Air Force C^3I Systems," *Seminar on Command, Control, Communications and Intelligence, Spring 1982* (Cambridge, Mass.: Program on Information Resources Policy, Harvard Univ., 1982), p. 105.

3. Comment based upon views expressed by Mr. Craig Wilson, director of Intelligence Training, Office of the Secretary of Defense, in a January 1988 interview.

4. Bob Brewin, "NSA Keeps Equipment from Guard," *Federal Computer Week* 2, no. 17 (25 April 1988) 1.

5. Ibid.

6. Ibid.

7. Ralph Vartabedian, "Pentagon's 'Black Programs' Leave Financial World in the Dark," *Washington Post*, 10 April 1988, sec. H.

8. Ibid.

9. Mark Thompson, "Army Drone Plagued by Problems," *Philadelphia Inquirer* (13 January 1988) 1.

10. James Bernstein, "Grumman's Radar Work Hits a Second Snag," *Long Island Newsday*, 13 January 1988, p. 47.

11. Lt. Gen. John H. Cushman (U.S. Army ret.), *Command and Control of Theatre Forces: Adequacy* (Washington, D.C.: AFCEA Press, 1985), p. 2-48.

12. Ibid., p. 2-47.

13. Ibid., p. 2-19.

14. VADM Jon L. Boyes (USN ret.), "BICES: Linking NATO Intelligence," *Signal* 42, no. 2 (October 1987) 20.

15. Eckersley-Maslin, RADM (Royal Navy ret.) D.M., "NATO C^3: An Achievable Goal," *Signal* 42, no. 2 (October 1987) 53.

16. "USAF Pursues Standardized Allied Reconnaissance Data," *Aviation Week and Space Technology* (21 September 1987) 25.

17. *Executive Order 12333*, 4 December 1981, The Federal Register, p. 59953.

18. Comments made by Mr. Craig Wilson, director of Intelligence Training for the Office of the Secretary of Defense, in an interview conducted in January 1988.

APPENDIX A

THE ROLES OF INTELLIGENCE

The roles of intelligence have been categorized in many different ways but are generally considered as a set of elements consisting of clandestine collection, counterintelligence, analysis and estimates, and covert action.[1] Each of these has relevance to the employment of military force. Let's consider them individually.

CLANDESTINE COLLECTION

Clandestine collection is defined as obtaining information of national security significance through either human or technical means. The information may be used by the government, the military, or individuals.[2] The collection of information about an enemy's forces, movements, disposition, and intentions can be critical as a "force multiplier" either strategically or tactically. Current military doctrine and strategy, as we will discover in appendix B, is very dependent upon information of enemy activity for success.

Collection of information is done through a variety of means. Human intelligence (HUMINT) refers to obtaining information through human sources. Insight provided by defectors, expatriates, or other human sources often provides useful information about enemy capabilities or intentions.[3]

Electronic intelligence (ELINT) is information gained through the interception of foreign electromagnetic emissions, noncommunications in nature, emanating from other than nuclear radiation or radioactive sources.[4] ELINT includes information about enemy electronic system capabilities.

Another form of intelligence collection is the interception of telecommunications transmissions, including data picked up from highly-sophisticated receivers. This type of signals manipulation is often referred to as signals intelligence (SIGINT).[5]

COUNTERINTELLIGENCE

Counterintelligence (CI) activities include friendly "neutralizing" actions taken to counter the intelligence efforts of another government or group. CI includes friendly activities that expose the plans or intentions of another government or group. Counterintelligence may also refer to the "manipulation" of an opposing intelligence service through deception.[6]

The term counterintelligence implies a "defensive" nature to these activities. This implication is not an accurate one. CI may actually negate an adversary's hostile intelligence actions. The implication of "passivity" in such actions is misleading. Indeed, CI can prove to be just as valuable for the outcome of friendly actions as other forms of intelligence perceived to be more "active" in their nature.[7]

ANALYSIS AND ESTIMATES

Analysis and estimates is the function of processing information obtained from collection or counterintelligence for presentation to decision makers of a product of greater clarity than the original data itself.[8] Estimates can take various forms. The CIA's *National Intelligence Daily* provides important information for the president. The DIA's *Defense Intelligence Daily* does the same thing for the secretary of defense. Estimates also include in-depth studies such as the National Intelligence Estimates, which are provided as coordinated policy documents.[9]

COVERT ACTION

Covert action is the act of influencing the actions of other individuals, groups or states without revealing one's involvement.[10]

Covert intelligence actions have received a lot of attention in the last few years. The "morality" of this kind of activity has been raised often. When these activities have been exposed, questions of ethics, legality, and rights to privacy have been dissected in the media, in public debates of Congress, and in the many books which have been written. As controversial as these subjects may be, they are not of prime concern to the battle manager. There is little argument with the military tactician that covert activity (or any other "role" of intelligence) can influence the outcome of a military action, particularly when it is a coordinated segment of the action itself.

The emphasis of this paper is the tactician's concern. The elements of intelligence have direct application to military battle management and force employment decision making.

NOTES

1. Roy Godson, *Intelligence Requirements for the 1980s, Elements of Intelligence*, National Strategy Information Center, Washington, D.C., 1983, pp. 6-8 (hereafter, Godson, *Elements of Intelligence*).

2. Ibid., p. 6.

3. Roy Godson, *Intelligence Requirements for the 1980s, Number 5, Clandestine Collection*, National Strategy Information Center, Washington, D.C., 1982, p. 11.

4. Ibid., article by Amrom Katz, p. 102.

5. Ibid.

6. Godson, *Elements of Intelligence*, p. 8.

7. Roy Godson, *Intelligence Requirements for the 1980s, Number 3, Counterintelligence*, National Strategy Information Center, Washington, D.C., 1980, paper by Arthur A. Zuehlke, Jr., pp. 13-14.

8. Godson, *Elements of Intelligence*, p. 7.

9. Ibid.

10. Ibid., p. 8.

APPENDIX B

THE INTELLIGENCE COMMUNITY

The intelligence community consists of the following agencies: the CIA, the Department of Treasury, the Department of Commerce, the FBI, the Department of State, the Department of Energy, the NSA, the DIA, and the military services. We will look briefly at the roles performed by these agencies and their individual mission taskings.

CENTRAL INTELLIGENCE AGENCY

The Central Intelligence Agency, at least from a statutory standpoint, is among the oldest intelligence organizations in the United States government. Its origins can be traced to the Office of Strategic Services (OSS) of World War II and the OSS's founder, General "Wild Bill" Donovan. In an attempt to handle the war's intelligence needs, Donovan had submitted as early as 1944 that outlined a post-war plan for attempting to streamline the structure of the six major and countless splinter groups that had sprung up over the course of the war.[1]

Donovan's Plan was eventually translated into a plan submitted to President Truman in 1946 by the Joint Chiefs of Staff (JCS). The basic intent was aimed at centralizing the various intelligence functions under a civilian agency. One of the primary concerns that had to be addressed at the time was the question of civil or military control of the national intelligence assets. The issue was not resolved completely until 1953 when the position of deputy director of Central Intelligence (DDCI) was created. When this was done, the stipulation was made that a military person could be appointed only to the position of director or deputy director at a given time. Civilian control of national intelligence was thus assured.[2]

Today, the mission of the CIA is defined in the president's *Executive Order 12333*. Specifically, the tasking of the Central Intelligence Agency is to

- Collect, produce and disseminate foreign intelligence and counterintelligence, including information not otherwise obtainable.

- Conduct counterintelligence activities outside the United States . . . . Conduct counterintelligence within the Unites States in coordination with the FBI as required by procedures agreed upon the Director of Central Intelligence and the Attorney General.

- Coordinate counterintelligence activities . . . when conducted outside the United States by other departments and agencies.

- Conduct special activities approved by the President. No agency except the CIA . . . may conduct any special activity unless the President determines that another agency is more likely to achieve a particular objective.

- Carry out or contract for research, development and procurement of technical systems and devices related to authorized functions.[3]

DEPARTMENT OF TREASURY

The Treasury Department has the responsibility to "overtly collect foreign financial and monetary information."[4] The Department, through its office of Intelligence Support and in conjunction with the State Department, "overtly collects foreign economic, financial, and monetary data."[5] Finally, the Treasury Department's Secret Service is tasked with conducting "activities to determine the existence and capability of surveillance equipment being used against the President."[6]

DEPARTMENT OF COMMERCE

The Commerce Department has become involved more in the intelligence business in recent years. The Department's prime concern is with the transfer of critical technology through unauthorized export. Commerce's office of Intelligence Liaison receives intelligence information from throughout the intelligence community relating to technology transfer. In addition, the Department's office on Export Enforcement insures "that the proper approvals have been obtained for the export of sensitive technology and to prevent unauthorized shipments of such technology."[7]

FEDERAL BUREAU OF INVESTIGATION

The history of the Federal Bureau of Investigation (FBI) is as colorful as its most famous director, J. Edgar Hoover. A great deal has been written about Hoover's attempts to expand the role of the FBI into the foreign intelligence arena. The squabbling that went on between Hoover and the World War II head of the OSS, "Wild Bill" Donovan, finally led President Roosevelt to divide the responsibilities of the two agencies geographically, with the FBI having foreign intelligence responsibility for the Western Hemisphere.[8] The National Security Act and subsequent legislation and executive orders has changed all of that.

Today, the director of the Federal Bureau of Investigation operates under the supervision of the Attorney General, and his responsibilities remain focused on two primary areas -- domestic counterintelligence and criminal law enforcement. *Executive Order 12333* does allow the FBI to engage in "counterintelligence activities outside the United States in coordination with the CIA."[9]

DEPARTMENT OF STATE

Intelligence activity of the State Department is conducted primarily by the Bureau of Intelligence and Research (INR). The Bureau is not engaged in any collection efforts other than its use of information available in open or normal diplomatic sources. The Bureau produces a *Morning Summary*, designed to inform the Secretary of State and his deputies of current intelligence.[10] The Secretary of State functions as a member of the National Security Council and therefore has input to intelligence priorities. In addition, the Department of State is directed to

- Overtly collect information relevant to U.S. foreign policy concerns.
- Produce and disseminate foreign intelligence relating to the United States' foreign policy as required for the execution of the Secretary's responsibilities.

- Disseminate, as appropriate, reports received from the United States' diplomatic and consular posts.[11]

DEPARTMENT OF ENERGY

The Department of Energy (DOE) "participates with the Department of State in overtly collecting information with respect to foreign energy matters."[12] DOE's assistant secretary for International Security Affairs has a Defense Intelligence Division which fulfills this intelligence responsibility. This division also manages the Lawrence Livermore Laboratory, which provides analysis of nuclear weapons technology and the technology's world-wide proliferation.[13]

DEPARTMENT OF DEFENSE

The Department of Defense (DOD) has the primary responsibility for the collection, production, and dissemination of military and military-related intelligence for the U.S. The secretary of defense is in the position of "owning" the largest share of intelligence resources in the United States. Although this appears to be the case, it is a little misleading. The National Security Agency is considered a "national" asset. Even though this organization is included under the DOD on organization charts, its tasking and control does not really lie within DOD. Let's look briefly at the Defense Department's portion of the "intelligence community."

NATIONAL SECURITY AGENCY

The NSA has been called N(ever) S(ay) A(nything)[14] because of the secrecy which has surrounded the agency virtually since its birth. The origin of the NSA is indeed unique. Its predecessor, the Armed Forces Security Agency (AFSA), suffered from the same types of problems that plagued the OSS: inter-service rivalry. Although the AFSA was "under the direction of the JCS," the agency was run by its director, who spent

a great deal of his time negotiating with the three services in order to accomplish the agency's taskings.[15] On 24 October 1952, President Truman signed a memorandum which was sent to his Secretaries of State and Defense. The memo directed the establishment of the National Security Agency, effective 4 November 1952.[16] The memo itself was classified, and the knowledge of its existence and the agency it created were kept secret for several years.

Since this beginning, the NSA has grown into one of the largest organizations in the government. From its headquarters at Fort Meade, Maryland, the NSA acts as the "single manager" for all signals intelligence activities of the intelligence community and is the executive agent for the communications security (COMSEC) programs within the government.[17] As a "national" agency, the NSA takes much of its operational direction from the DCI.

DEFENSE INTELLIGENCE AGENCY

The trend toward centralization of the intelligence business which led to the creation of both the CIA and NSA continued through the 1950s and into the early 1960s. The Defense Intelligence Agency (DIA) was the next organization created in an attempt to better centralize military intelligence activities. It was established on 1 August 1961 by a DOD directive. Its purpose was to act as a consolidating agency for the management of all DOD intelligence resources. [18]

The DIA is really an agency created out of a compromise related to ownership of the agency itself. When the DIA was created, there were two schools of thought. The defense secretary (McNamara) wanted an agency which was under the direct control of policy makers. The JCS wanted an agency which would be organized under them and function as a "Joint Military Intelligence Agency." A compromise was agreed upon. The DIA reports through the JCS to the secretary of defense and functions as the intelligence staff element for the JCS.[19] This arrangement is still in effect today.

The tasking of the DIA has also remained relatively unchanged. The DIA is responsible for

- Collection, production, or, through tasking and coordination, provision of military and military-related intelligence for the Secretary of Defense.
- Collection and provision of military intelligence for national foreign intelligence and counterintelligence products.
- Coordination of all Department of Defense intelligence collection requirements.[20]

SERVICE INTELLIGENCE ACTIVITIES

As was true in World War II, the military services continue to possess a considerable staff and force structure devoted to military intelligence. As with the other intelligence agencies, the foreign intelligence and counterintelligence elements of the services have taskings found in the president's *Executive Order 12333*. Specifically, they include

- Collection, production and dissemination of military and military-related foreign intelligence and counterintelligence. . . . When collection is conducted in response to national foreign intelligence requirements, it will be conducted in accordance with guidance from the Director of Central Intelligence.
- Conduct of counterintelligence activities outside the United States in coordination with the CIA.
- Monitoring of the development, procurement and management of tactical intelligence systems.[21]

Each of the service's intelligence functions has its own set of responsibilities. Army intelligence collects, produces, and disseminates military and military-related foreign intelligence and operates its own tactical intelligence systems. The Navy conducts specialized collection and analysis related to the Naval environment. The Air Force collects intelligence to satisfy both Air Force and national needs. It possesses the largest intelligence component of the services, and its Foreign Technology Division provides the leading source of analysis of foreign aircraft and missiles.[22]

NOTES

1. Thomas F. Troy, *Donovan and the CIA: A History of the Establishment of the Central Intelligence Agency*, Aletheia Books, University Publications of America, Inc., 1981, pp. 209-229.

2. Ibid., pp. 408-410.

3. *Executive Order 12333*, 4 December 1981, The Federal Register, vol. 46., no. 235, Tuesday, 8 December 1981, pp. 59945-59946 (hereafter, *Executive Order 12333*).

4. Ibid., p. 59946.

5. Jeffrey Richelson, *The U.S. Intelligence Community* (Cambridge, Mass.: Ballinger Publishing Company, 1985), p. 100 (hereafter, *The U.S. Intelligence Community*).

6. *Executive Order 12333*, p. 59946.

7. *The U.S. Intelligence Community*, p. 99.

8. Ibid., p. 103.

9. *Executive Order 12333*, p. 59949.

10. *The U.S. Intelligence Community*, p. 96.

11. *Executive Order 12333*, p. 59946.

12. Ibid., p. 59949.

13. *The U.S. Intelligence Community*, pp. 100-101.

14. "Never Say Anything," *National Journal* (31 October 1987): 2717.

15. James Bamford, *The Puzzle Palace: A Report on America's Most Secret Agency*, R.R. Donnelly & Sons Company, Harrisonburg, Virginia, 1982, pp. 77-78.

16. Ibid., p. 81.

17. *Executive Order 12333*, pp. 59947-59948.

18. *The U.S. Intelligence Community*, pp. 35-36.

19. Ibid.

20. *Executive Order 12333*, p. 59947.

21. Ibid., pp. 59948-59949.

22. Scott D. Breckinridge, *The CIA and the U.S. Intelligence System*, Westview Press, 1986, p. 49.

APPENDIX C

THE INTELLIGENCE "PRIORITY-SETTERS"

The setting of intelligence priorities is important when you consider the "ownership rights" are spread among so many different agencies. In this appendix, we will briefly look at the "players" who set both "national" and "military" intelligence priorities.

PRESIDENT

The president is the ultimate "priority setter." As head of the Executive Branch and the nation's military, the president has the authority to set intelligence priorities (within the confines of the law). Ultimately, the decision on intelligence resource allocation may have to go to the president for final resolution.

NATIONAL SECURITY COUNCIL

The National Security Council, acting as the president's senior advisory staff, assists the president in forming intelligence priorities and policies. The director of Central Intelligence is in regular attendance at meetings of the NSC and, in turn, acts as the NSC's intelligence advisor. In the Reagan Administration, the NSC's intelligence policy formulation function has been handled through the NSC's Senior Interagency Group (SIG) (Intelligence). This group is composed of the DCI, the president's national security advisor, the director of the NSA, the director of the FBI, the chairman of the JCS, the deputy secretaries of State and Defense, and the deputy attorney general.

DIRECTOR OF CENTRAL INTELLIGENCE

The director of Central Intelligence, as the title implies, is the central figure in the U.S. intelligence community. He has statutory authority to set the priorities of virtually every agency involved in the collection of foreign intelligence and counterintelligence information collected outside the United States. He is responsible for the management of the intelligence budget, which applies to all "national" assets, even those falling under the "control" of the secretary of defense.[1]

The orientation of the DCI has varied through changes in administrations and as the DCI's themselves have changed. It has been written that

> DCI's have three orientations: They approach their task as that of *head* of the CIA, *coordinator* of the intelligence community, or the principle intelligence *advisor* to the President.[2]

Over the years, different individuals have taken each of these orientations. For example, Alan Dulles, DCI during the Eisenhower years, had a strong background in the OSS of World War II. As a result, covert operations dominated his involvement as DCI. John McCone, who served under President Kennedy, was seen as a policy advocate "with the intent of becoming a power in the administration." Richard Helms, who served as DCI from 1966 until 1973, emphasized loyalty to the profession of intelligence and to the CIA as an organization. William Colby, who followed Helms as the DCI, was seen by some members as a traitor to the intelligence business for releasing so much information to the Church Committee in the investigations of the CIA in the mid-1970s. George Bush was seen as a DCI who was loyal to the president and the administration. Finally, William Casey's tenure was characterized as being dominated by zealous support of the struggle against communism in Central America and terrorism in the Middle East.[3]

SECRETARY OF DEFENSE

The secretary of defense (SECDEF) is both "customer" of and "priority setter" for intelligence resources. As the president's military czar, the SECDEF can influence the priority for intelligence and act as the voice of field commanders for intelligence resource allocation.

DIRECTOR OF DIA

The director of the DIA is not a major player in the setting of priorities for either the collection or dissemination of intelligence, certainly not in the same way as the DCI or even the director of the NSA. The DIA acts as a coordinator of intelligence gathered by the services and a staff element for intelligence for the JCS. The director of the DIA is also responsible for the management of the Defense Attache system.[4]

NOTES

1. Robert D. Beland, *The National Foreign Intelligence Program/Budget Process*, Defense Intelligence College, undated; and *Executive Order 12333*, p. 59944.

2. Glenn Hastedt, "Controlling Intelligence: The Role of the D.C.I.," *International Journal of Intelligence and Counterintelligence* 1, no. 4 (1987): 27.

3. Ibid., pp. 30-39.

4. *Executive Order 12333*, Federal Register, p. 59947.

APPENDIX D

THE MILITARY "OPERATORS"

Military operations can involve many "players," each with their own set of functional missions. In this appendix, we will review the organizational structure which has been created to fulfill U.S. force employment responsibilities.

PRESIDENT

The Constitution establishes the president as the Commander-in-Chief of the Armed Forces and provides for his authority for the employment of those forces. Legislation such as the War Powers Act now requires the president to justify many actions which he may undertake with respect to military force employment for Congressional oversight. The fact remains, however, that the president is the individual who provides the ultimate force employment direction.

NATIONAL SECURITY COUNCIL

The National Security Council was established by the National Security Act of 1947. Its role in force employment has varied since its creation. Under President Eisenhower, the NSC went through a period of relatively smooth operation. During this period, the NSC functioned primarily as a national strategy forum. With other administrations, the role of the NSC changed. Under Presidents Kennedy and Johnson, the NSC's national strategy function began to move more into operational involvement and decision making.[1] Much more recently, the extent of this change in direction of the NSC role into "operations" has been well-publicized through the events of the Iran-Contra affair.

Primary membership of the NSC consists of the president, the vice president, the secretary of state, and the secretary of defense. The chairman of the Joint Chiefs of Staff, the special assistant to the

president for National Security Affairs, the director of Central Intelligence, the secretary of treasury, and the director of OMB also attend NSC meetings (others may be invited upon request).[2] Its function during crisis or war will most likely continue to vary with future presidents. It seems a logical role for future NSCs to serve as the president's operations staff providing "independent advice integrating military considerations in the larger perspective of national strategy."[3]

SECRETARY OF DEFENSE

The position of secretary of defense (SECDEF) was established by the 1949 amendment to the National Security Act of 1947. The SECDEF provides the day to day civilian control of the U.S. military. The SECDEF has the responsibility for both the operational (represented by the Unified and Specified Commands) and support (represented by the military services) segments of the military. The secretaries of the Army, Navy, and Air Force support the SECDEF in the administration of service programs while the Joint Chiefs of Staff serve as the SECDEF operational advisors.

JOINT CHIEFS OF STAFF

The Joint Chiefs of Staff (JCS) were established as the principal military advisors to the president by the National Security Act of 1947. The JCS is composed of the chiefs of staff of the Army and Air Force, the chief of Naval Operations, and the commandant of the Marine Corps. The size of the JCS has been limited to 400 since the 1958 amendment to the National Security Act was passed.

Most recently, some changes to the JCS have been mandated by the Goldwater-Nichols DOD Reorganization Act of 1986 (P.L. 99-433). Many of these changes are addressed at the power of the chairman of the JCS. Specifically, the chairman is tasked to act as "the principle military advisor to the President, the National Security Council, and the

Secretary of Defense." In addition, the chairman is not required to obtain a consensus from the entire JCS prior to offering his advise to the president. He is only required to

> as he considers appropriate, inform the President, the National Security Council, or the Secretary of Defense, as the case may be, of the range of military advise and opinion with respect to that matter.[4]

The statute allows other members of the JCS to provide advice to the president, NSC, or SECDEF "on a particular matter when the President, the National Security Council, or the Secretary requests such advice."[5]

The Act created the (new) position of vice chairman of the JCS. The vice chairman is designated to "function as Acting Chairman"[6] and to vote as chairman "when acting in that capacity."[7] The law places the vice chairman as senior in rank to the other members of the JCS (except the chairman) and establishes the vice chief as immediately behind the chairman in the order of succession.[8]

UNIFIED AND SPECIFIED COMMANDERS

The military forces' operational arms are organized into several unified (consisting of two or more services) and specified (consisting of one service) commands, which have been established "to accomplish a broad continuing mission" under a single commander (whose chain of command runs "from the President to the Secretary of Defense; and . . . from the Secretary of Defense to the commander).[9] These commands may be multinational, the U.S. element of a larger multinational command, or a U.S.-only command. They have been delegated the operational responsibility to perform some part of the nation's military mission. The commands are the ultimate military "operational users" of information gathered by the U.S. intelligence community.

STRATEGIC AIR COMMAND

The Strategic Air Command (SAC), headquartered at Offutt Air Force Base, Nebraska, is a specified command with a specific *functional* tasking. SAC has the mission responsibility of providing the strategic strike capabilities of our nation employing manned bombers and Intercontinental Ballistic Missiles (ICBMs). SAC's forces comprise two-thirds of the U.S. strategic TRIAD. SAC has some additional responsibilities. The CINCSAC is also the commander of the Joint Strategic Connectivity Staff. This organization is responsible for ensuring the continuity of command and control of strategic forces in the event of nuclear war through the trans- and post-attack periods. CINCSAC's third "hat" is the one he wears as the commander of the Joint Strategic Target Planning Staff. This staff, taking guidance from the president and secretary of defense through the Joint Chiefs of Staff, develop the National Strategic Targets List and, in turn, the Single Integrated Operations Plan.[10]

NORTH AMERICAN AEROSPACE DEFENSE COMMAND

The North American Aerospace Defense Command (NORAD) is a multinational command that is supported by a U.S. specified command, Aerospace Defense Command. The command, originally called the North American Air Defense Command, has existed as a joint venture of the U.S. and Canada since 1957. The mission tasking of NORAD has remained relatively unchanged since its inception. From its headquarters at Cheyenne Mountain, Colorado, NORAD is tasked with the defense of the North American continent against the air breathing threat (manned bombers and cruise missiles).[11]

AIR FORCE SPACE COMMAND

Also having its headquarters at Cheyenne Mountain is the Air Force Space Command. This specified command was established 1 September 1982 and is responsible for the warning of attack on the North American

continent by ballistic missiles and for cataloguing and tracking thousands of objects now orbiting the earth. Space Command is also responsible for nuclear detection monitoring and weather reconnaissance and manages two satellite programs, the Defense Support Program (DSP) and the Defense Meteorological Satellite Program (DMSP). The DSP is responsible for the detection of missile launches, space launches, and nuclear detonations and the DMSP provides weather information for military use.

The commander of NORAD also functions as the commander of Air Force Space Command and Aerospace Defense Command.[12]

U.S. TRANSPORTATION COMMAND

The U.S. Transportation Command (USTRANSCOM) was established on 18 April 1987. The command is among the newest of the unified commands and is headquartered at Scott AFB, Illinois. Proposals for this command date back to 1955; however, the current command arrangement was created as a result of the Packard Commission, a presidential blue ribbon panel.[13]

National Security Decision Directive (NSDD) 219 directed the formation of single unified command to "provide global air, land, and sea transportation" for the military.[14] USTRANSCOM was the result.

The complete "development" of the USTRANSCOM will not occur until 1988, at the end of the four-phase implementation period which began in spring of 1987. When fully operational, the command "will give the Defense Transportation System one CINC."[15] The primary purpose of the planned organization is to join the resources of the Air Force's Military Airlift Command (strategic airlift assets), the Navy's Military Sealift Command (strategic sealift assets), and the Military Traffic Management Command (MTMC), which is responsible primarily for ocean terminal operations and liaison between defense and commercial shippers.[16]

ATLANTIC COMMAND

One of two "ocean" commands, Atlantic Command (LANTCOM) maintains its headquarters at Norfolk, Virginia, and is considered "unified" in its structure. It is among the oldest of the operational commands with its history dating back to 1947. The commander of LANTCOM (CINCLANT) is also the commander of the Atlantic Fleet (CINCLANTFLT). Although designated a unified command, it has never had any Army or Air Force units permanently assigned to it. Instead, the Air Force's Tactical Air Command and the Army's Forces Command (FORSCOM) are considered "component" commands of LANTCOM and would provide forces to LANTCOM on a more or less ad hoc basis in the event of hostilities.[17]

U.S. PACIFIC COMMAND

U.S. Pacific Command (PACOM) is the second of the U.S.'s ocean commands and is unified in its structure. As with LANTCOM, PACOM has its roots with the Unified Command Plan signed by President Truman in 1946.[18] PACOM has its headquarters at Camp Smith, Hawaii, and has been traditionally commanded by a four-star Navy admiral.[19]

PACOM has two major and one lesser subordinate component commands. The Navy component, CINCPACFLT, is also commanded by a four-star admiral. Unlike CINCLANT, CINCPAC does not dual-hat as CINCPACFLT. The Air Force's component is the Pacific Air Force, or PACAF. The Army component of PACOM has been delegated to an organization called WESTCOM, or Western Command.[20] The PACOM Area of Responsibility extends from 100 degrees east to 95 degrees west in the north, and 17 degrees east to 92 degrees west in the south. The area covers the Indian Ocean, parts of Africa, India, Australia, Japan, China, Korea, parts of the Soviet Union and Alaska, and portions of the U.S., Canada, and Mexico.[21]

U.S. EUROPEAN COMMAND

U.S. European Command (EUCOM) is the U.S. unified command element of the Allied Command, Europe, a multinational operational command. EUCOM headquarters is in Stuttgart, West Germany. The Supreme Allied Commander, Europe (SACEUR) is also the commander of EUCOM.[22] The origins of EUCOM also go back to the Unified Command Plan of 1946.

The command arrangement in Europe is among the most complicated and yet simplest in existence. The command is complicated by the fact that the multinational aspects of the command arrangement exist even in the subordinate commands under SACEUR and simplified by the fact that many of these commands are "dual-hatted." For example, the peacetime Army component commander, CINC, U.S. Army Europe becomes the commander of the Central Army Group of the Allied Forces Central Europe of the Allied Command, Europe, in war. Also, the commander of the U.S. Air Forces Europe (USAFE) becomes the commander of the Allied Air Forces Central Europe (AAFCE) during war.[23] This command arrangement is only one of many factors which make the European theatre unique from a force employment perspective. This theatre is discussed in greater detail in chapter 3. We will discuss some factors which impact the intelligence and operations functions in Europe, complicate the optimum operations to intelligence functional marriage, and jeopardize the Allied chances of success during a potential conflict.

U.S. SPECIAL OPERATIONS COMMAND

The United States Special Operations Command (USSOCOM) was established on 16 April 1987 and activated on 1 June 1987. This command is headquartered at MacDill Air Force Base, Florida, and is unique in many respects. USSOCOM is a replacement for the U.S. Readiness Command (earlier called Strike Command) and came about as a result of the Goldwater-Nichols DOD Reorganization Act of 1986. This legislation mandated a study to determine the need for a Special Operations Command designed to deal specifically with low intensity warfare. The study

produced as a result of Goldwater-Nichols was the Joint Low Intensity Conflict Project, released in August 1986. Although the recommendations of this study are still classified, the USSOCOM was established as a rider on the FY 1987 Defense Appropriations Bill. The Command's existence was thus Congressionally mandated.[24]

The USSOCOM's mission is "to provide combat-ready special operations forces for rapid reinforcement of other unified commands."[25] USSOCOM is also responsible for the joint training of the forces assigned to it as well as the planning and execution of special operations directed by the president or secretary of defense.[26] Forces assigned to the USSOCOM are elements of the Army First Special Operations Command, the 23rd Air Force, the John F. Kennedy Special Warfare School, Navy Special Warfare Center, the USAF Special Operations School, the Reserve and Guard Special Operations Forces, and the Naval Special Warfare School.[27]

This command arrangement represents the latest in the attempts to deal with the problem of low-intensity conflict, which was glaringly revealed in 1980 with failure of the Iran hostage rescue attempt.[28]

U.S. SOUTHERN COMMAND

United States Southern Command (USSOUTHCOM) is a unified command with specific geographic responsibilities. The command is responsible for the Central and South American areas.[29] It has its headquarters at Quarry Heights, Panama.[30]

U.S. CENTRAL COMMAND

United States Central Command (USCENTCOM) is another of the unified commands with specified geographic taskings. Central Command was established in January 1983 and replaced the Rapid Deployment Force. It has its headquarters at MacDill Air Force, Florida, and has the countries of the Middle East, Northeast Africa, and Southwest Asia. Central Command's area of responsibility includes the Persian Gulf,

Afghanistan, and Pakistan to the east; Egypt, Somalia, and Sudan to the West; the Indian Ocean to the south; and Turkey and the Soviet Union to the north. [31]

SERVICES

The services have important but clearly different responsibilities than the operational commands mentioned above. The Army, Navy (and its Marine Corps "component"), and Air Force are tasked with "organizing, training and equipping" the military forces of this country. These departments have no war-fighting responsibilities but do have enormous influence on the capabilities of the combatant commands to accomplish their missions. By holding the "purse strings" of the military, the services virtually direct the capability which is then made available for use by the "field commanders." The services also develop their own strategies and doctrine under which the field commanders are then directed to operate. In effect, the services own the forces the field commanders may be given for operational control -- and tell these commanders, in broad terms, how they will fight.

Much has been written about the relationship of the services to the field commanders. Perhaps no one expressed the concerns of this arrangement better than retired General John Cushman in his book, *Command and Control of Theatre Forces: Adequacy*. In discussing the institutional causes of the failure of the "system" to provide the field commander with well-conceived and integrated command and control systems, he said:

> First is the failure of the Service provider to look holistically at the operational commander's entire web of command and control. This stems from the narrowly based, Service-oriented outlook which comes naturally and institutionally to a Service and which is most difficult to eradicate.[32]

NOTES

1. Carnes Lord, "Rethinking the NSC Role," *Comparative Strategy: An International Journal* 6, no. 3 (1987): 246-247.

2. Scott D. Breckinridge, *The CIA and the U.S. Intelligence System*, Westview Press, 1986, chart on p. 15.

3. Ibid., p. 273.

4. P.L. 99-433, *Goldwater-Nichols DOD Reorganization Act of 1986*, 1 October 1986, p. 100 STAT. 1005.

5. Ibid.

6. Ibid., p. 100 STAT. 1009.

7. Ibid.

8. Ibid.

9. Ibid., p. 100 STAT. 1013.

10. Jeffrey Richelson, *The U.S. Intelligence Community* (Cambridge, Mass.: Ballinger Publishing Company, 1985), p. 76 (hereafter, *The U.S. Intelligence Community*).

11. Lt. Gen. John H. Cushman, *Command and Control of Theatre Forces: Adequacy* (Washington, D.C.: AFCEA Press, 1985) chapter 2 (hereafter, *Adequacy*).

12. Ibid., p. 78.

13. *Airlift: The Journal of the Airlift Operations School* 9, no. 3 (Fall 1987): 1.

14. Ibid.

15. Ibid., pp. 4-5.

16. Ibid., pp. 6-7.

17. *Adequacy*, pp. 3-34 to 3-35.

18. Ibid., p. 3-20.

19. Ibid., pp. 3-36 to 3-35.

20. Ibid., p. 3-35.

21. *The U.S. Intelligence Community*, p. 80.

22. *Adequacy*, pp. 3-5 to 3-7.

23. *Adequacy*, pp. 3-29 to 3-30.

24. Kenneth Brooten, Jr., "The U.S. Special Operations Command: Armed Forces Unite to Counter the Reality Low Intensity Conflict," *Journal of Defense and Diplomacy* 5, no. 10 (1987): 21-22.

25. Ibid., p. 23.

26. Ibid.

27. Ibid.

28. Ibid.

29. *The U.S. Intelligence Community*, p. 82.

30. *Adequacy*, p. 3-6.

31. *The U.S. Intelligence Community*, p. 81.

32. *Adequacy*, p. ES-5.