Incidental Paper

Seminar on Command, Control, Communications and Intelligence

Student Papers — Spring 1980

C. Kenneth Allard
George N. Curuby
Kenneth Freeman
Newell Highsmith
Thomas Leney
David C. McGaffey
Marc Dean Millot

Program on Information Resources Policy

Harvard University

Center for Information Policy Research

Cambridge, Massachusetts

An incidental paper of the Program on Information Resources Policy.

SEMINAR ON COMMAND, CONTROL, COMMUNICATIONS AND INTELLIGENCE.
Student Papers - Spring 1980: C. Kenneth Allard, George N. Curuby, Kenneth Freeman, Newell Highsmith, Thomas Leney, David C. McGaffey, Marc Dean Millot.
January 1981. I-81-1.

Printing 5 4 3 2 1

Contributors

Action for Children's Television
Association of American Publishers
American Broadcasting Companies, Inc.
American District Telegraph Company
American Telephone & Telegraph Co.
Arthur D. Little Foundation
Auerbach Publishers Inc.
Automated Marketing Systems
Bell Canada (Canada)
Beneficial Management Corporation
Albert Bonniers Forlag AB (Sweden)
Boston Broadcasters, Inc.
The Boston Globe
Booz-Allen Hamilton
Burroughs Corporation
Cable and Wireless, Inc.
Canada Post (Canada)

CBS Inc.
Central Telephone & Utilities Corp.
Citibank N.A.
Codex Corporation
Communications Workers of America
Computer & Communications Industry Assoc.
Continental Telephone Corporation
Des Moines Register and Tribune Company
Direction Générale des Télécommunications (France)
Donaldson, Lufkin and Jenrette
Doubleday, Inc.
Dow Jones & Co., Inc.
Dun & Bradstreet
Economics and Technology, Inc.
Elsevier Science Publishers (Netherlands)
Encyclopaedia Britannica
L. M. Ericsson (Sweden)
Exxon Enterprises, Inc.

Federal Reserve Bank of Boston
First National Bank of Boston
First National Bank of Chicago
France Telecom (France)
Frost & Sullivan
General Electric Company
General Telephone & Electronics
Hallmark Cards, Inc.
Hambrecht & Quist
Harte-Hanks Communications, Inc.
Hazel Associates
Honeywell, Inc.
Hughes Communication Services, Inc.
IBM Corporation
Information Gatekeepers, Inc.
International Data Corporation
International Paper Company
International Resources Development, Inc.
International Telephone & Telegraph Corp.
Italtel (Italy)
Knight-Ridder Newspapers, Inc.
Knowledge Industry Publications, Inc.
Lee Enterprises, Inc.
Lockheed Missiles and Space Company, Inc.
MCI Telecommunications, Inc.
McGraw-Hill, Inc.
Mead Data Central
Minneapolis Star and Tribune Company
MITRE Corporation
Motorola, Inc.
National Association of Letter Carriers
NCR Corporation
National Telephone Cooperative Assoc.
New York Times Company
Nippon Electric Company (Japan)
Norfolk & Western Railway Company

Pergamon Press Ltd. (United Kingdom)
Pitney Bowes, Inc.
Public Agenda Foundation
Reader's Digest Association, Inc.
Salomon Brothers
Satellite Business Systems
Scott & Fetzer Company
Seiden & de Cuevas, Inc.
Southern Pacific Communications Company
Standard Shares
St. Regis Paper Company
Swedish Television (Sweden)
Telesat Canada
Times Mirror Co.
Transamerica Corporation
The Toronto Star (Canada)
The Tribune Company

United Parcel Service
United States Government:
- Central Intelligence Agency
- Department of Commerce:
  - National Technical Information Service
  - National Telecommunications and Information Administration
- Department of Defense:
  - Defense Technical Information Center
- Department of Energy
- Federal Communications Commission
- National Aeronautics and Space Admin.
- National Security Agency

United States Postal Rate Commission
United States Postal Service
United Telecommunications
The Washington Post Company
Western Union
Western Union International, Inc.
Xerox Corporation

TABLE OF CONTENTS

Preface

On August 11, 1980 the New York Times reported that President Carter had issued three Presidential Directives (P.D. 53, 58 and 59) calling "for the study of several approaches to coping with a nuclear attack:

- Hardening command centers and communications posts by placing them underground or protecting them with concrete.

- Dispersing communications networks and making them redundant so that messages could continue to be sent after critical equipment was knocked out.

- Improving warning and evacuation techniques".

These concrete provisions apparently reflect heightened government attention to the nation's "nervous system", namely its command, control, communications and intelligence capabilities, relative to its "muscle", i.e., its weapons and the means for emplacing and using them.

Detailed elsewhere* is the broad significance of information resources as "social nervous systems", including their role in national and international security and their relation to "muscles". The Program on Information Resources Policy has focused attention on the organizing role of information resources in government and business through a graduate course on "Command, Control, Communications and Intelligence (C^3I) in Government and Business".

This course was first offered at Harvard's Kennedy School of Government in the spring of the 1979-80 academic year. It examined the changes

---

*Oettinger, Anthony G., "Information Resources: Knowledge and Power in the 21st Centure "Science, 209, pp 191-198, 4 July 1980.

since World War II in the conception, technologies and institutional framework of information resources and the implications of these changes for national security policy and linked domestic policies. The course and related Program research address the relationship between information resources and government policy choices or corporate strategic alternatives. They aim to fill a gap.

When not just relating war stories, most academic or professional approaches to intelligence emphasize political science or international politics but pay scanty attention to managerial, administrative or technological factors. Business schools and practitioners emphasize the techniques and the technicalities of management information systems (MIS), but they pay little attention to mutual influences between these and strategic goals. The Program's ultimate aim is to synthesize the best of both these approaches as well as to carry forward where both leave off.

In 1979-80 the students were exposed not only to faculty, but also to current or former government officials responsible--through several administrations--for recommending or carrying out decisions of the type reportedly made by President Carter: William E. Colby, of counsel, Reid & Priest; formerly Director of Central Intelligence. B. R. Inman, Director, National Security Agency and Chief, Central Security Service. William Odom, Military Assistant to the Assistant to the President for National Security Affairs. Lionel Olmer, Director of International Programs, Motorola, Inc.; formerly Executive Secretary, President's Foreign Intelligence Advisory Board. Lee Paschall, Consultant; formerly Director, Defense Communications Agency and Manager, National Communications System. Robert Rosenberg, Policy Assistant to the Assistant to the President for National

Security Affairs. Raymond Tate, Raymond Tate Associates; formerly Deputy Assistant Secretary of the Navy and Deputy Director of the National Security Agency. That students were exposed to only one business representative, A.K. Wolgast, Manager, Planning and Analysis Dept., Exxon International, reflects the gap between the aims of the course and their realization.

The student papers in this volume range across a variety of topics wide enough to indicate the scope of the problems before us. What they fail to address reveals the magnitude of the tasks still ahead.

The papers have been only lightly edited for consistency of format. Their substance is no more and no less than what each student contributed.

Anthony G. Oettinger

Introduction

The student papers in this volume explore relationships among three key aspects of private or public management:

1. the strategic goals of organizations;
2. the processes that decision makers use both to learn about the "outside" world (intelligence) and also to run and monitor their own organizations (command and control);
3. the technical means for carrying out intelligence, command and control processes in support of the formulation and the pursuit of strategic goals.

Although national and international security affairs provide most of the illustrations, with one example drawn from the oil industry, the generic findings should prove useful in managing for the survival and success of any organization.

Tom Leney's "Overview of Strategic Command, Control, Communications and Intelligence"(C^3I) draws on the planning to prevent or conduct a nuclear war to identify how strategic goals influence what is required of C^3I processes and of systems that will carry out these processes. In so doing he sets the stage for the other papers.

In the United States, the means for conducting war are conditioned by both the Constitution and, more immediately, by definitions of command authorities that are embodied in the National Security Act of 1947. Designed to respond to lessons learned in World War II, this law has stood without major amendment since 1958. What this means for C^3I in the 1980's is sketched by Newell Highsmith in "The Statutory Basis for the Authority of the National Command Authority."

How much to encourage and how much to restrict the flow of information is a perennial dilemma for all organizations. The dilemma is sharpened if, as in Billy Carter's Libyan affair, an official is "advised of extremely sensitive intelligence information". In the Carter instance, the Attorney General said that "My two most basic concerns were that in the absence of other sources any disclosure of the information could compromise the intelligence source; and, second, I did not want to abort the transaction, which might constitute substantial evidence of a duty to register under the Foreign Agents Registration Act".* Drawing on a wealth of World War II materials declassified within the past decade, Kenneth Freeman explores such dilemmas and other facets of the "Control of Sensitive Information."

Intelligence, like scholarship, is sometimes seen as an ornament more than a necessity. In particular, strategic intelligence is often seen as useful, if at all, only to top leadership but not to the troops in the trenches or the salesmen in the field. However, Tom Leney notes that "the growing importance of tactical military decisions to larger national interests [has] affected the degree of freedom local commanders are allowed to have". Conversely, the products of national intelligence--and note only what he can see through his binoculars--are of increasing significance and immediacy to a local commander, much as access by telephone to the home office's database is becoming to the insurance salesman out on a call. In "Re-shaping American Intelligence: Decisions for the 1980's", C. Kenneth Allard examines the organizational implications of these new relationships between strategic and tactical eyes, ears and memory.

---

* Department of Justice news release, August 6, 1980.

The visibility, glamour and expense of increasingly pervasive technical systems occasionally leads to forgetfulness about the human element in information flows, decision-making and commands. In Intelligence and Information Systems in the Department of State/Foreign Service, David C. McGaffey focuses on interaction, feedback, and trust, on cross-, up-, or down-channel effects, and on such tradeoffs as timeliness versus accuracy and accuracy versus usefulness. He explores the implications of various settings of these tradeoffs for organizational effectiveness and efficiency.

How the potential enemy--or the competition--organize themselves for command and control can provide valuable clues as to what one may himself expect to encounter. Since doctrine in the military, like standard operating procedures elsewhere, serves as a guide to action, it can then also serve to some extent, as a predictor of likely action. Drawing on U.S. military translations of Soviet works, Mark Dean Millot sketches The Soviet Doctrine of Troop Control.

Given the classified status of much sensitive military or intelligence information, some may find it odd that the public record on high-level government command, control and intelligence processes seems more extensive and explicit than the record of comparable business processes. This may stem from proprietary "classification", or perhaps from the fact that the institutionalization of C^3I processis is more extensive and that managerial (i.e., Congressial) oversight is more public in government than in business. The oil industry's reaction to Arab oil embargoes is a notable exception that George N. Curuby explores in Crisis Management at Exxon Corporation.

1. OVERVIEW OF STRATEGIC COMMAND, CONTROL, COMMUNICATIONS AND INTELLIGENCE

Tom Leney

TABLE OF CONTENTS

TABLE OF CONTENTS

INTRODUCTION

The purpose of this paper is to provide an overview command control, communications, and intelligence (often called "C-cubed-I") by examining the factors which influence C^3I requirements, the requirements themselves, and the qualities needed in C^3I systems to meet these requirements. Current systems will also be looked at in the context of these requirements in order to identify problems and issues that exist. The goal is to provide a basis upon which to assess current and future systems so that they may better meet the needs of national security. In order to limit the breadth of the subject somewhat, I shall focus on strategic C^3I, the means by which the nation's strategic nuclear forces are controlled and directed. If ICBM's, bombers, and missile submarines can be likened to our strategic nuclear "muscle" then strategic C^3I can be thought of as the nervous system that controls these muscles and coordinates their interaction to insure the accomplishment of desired tasks.

More formal definitions for the terms command, control, communications, and intelligence can be found in Department of Defense publications. There we find "command and control" defined as, "The exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of his mission."[1] The need to insure that only "properly designated commanders" can exercise authority, especially over nuclear forces, is a critical aspect of command and control. This concern has been a key factor influencing development requirements for command and control systems.

Communications is defined by the Department of Defense as, "The method or means of conveying information of any kind from one person or place to another except by direct unassisted conversation, or correspondence through non-military channels."[2] It is important to note that this definition does not exclude the use of commercial telecommunications networks. Most of the day-to-day communications within the military and the government use commercial systems and they provide a potentially valuable resource for re-establishing communications after an enemy nuclear attack. In view of the severe damage to communication systems that could be inflicted in a large scale nuclear attack, any and all options for getting messages from one location to another should be considered.

The term "intelligence" has several definitions. In its broadest sense it could include all external information gathered by government agencies. Executive Order 12036, which specifies the organization and control of intelligence provides a more useful definition which describes it as "information relating to the capabilities, intentions and activities of foreign powers, organizations and individuals."[3] For the purposes of this paper the definition of intelligence shall be further restricted to information gathered by surveillance systems that concerns the initiation of an enemy attack on the United States. The focus of this definition is on the acquisition of physical indications of an enemy attack (tactical warning) rather than the more complex task of determining enemy intentions. This is not to say that warning means merely saying "here they come," however; it includes all information concerning an attack that is relevant for making decisions concerning U.S. retaliation. (A more detailed discussion of warning can be found in the section, C^3I Functional Requirements.)

With these definitions in mind we shall first look at the four major factors that influence C^3I requirements. These are:

1) Strategic Doctrine - the way we plan to use our nuclear forces in response to an enemy attack;

2) Civilian Control - decisions regarding who should be able to direct the use of nuclear weapons affects the methods of command and control;

3) Enemy Threat - enemy capabilities that could affect the ability of the United States to respond to an enemy attack;

4) Technology - the hardware available for use in designing C^3I equipment and systems.

In the following sections, each of these factors will be examined to provide a framework for assessing C^3I requirements and determining how well current systems meet these requirements.

The impact of technology on C^3I systems will not be addressed explicitly, though it is obviously a very important consideration, as it is beyond the scope of this paper. Also, though technology is a major constraint on the ability of C^3I systems to meet the requirements placed on them, it is not as critical as the others in determining what requirements are desired. After we determine exactly what it is that we want a system to be able to do, then these specific requirements can be matched against available technology to get the best possible capability. Obviously design goals are limited by technological constraints but it is important to have them clearly articulated, understood, and challenged before looking at technology. Otherwise technology may determine requirements rather than requirements driving technology. When that happens, the phenomenon of "hardware looking for a mission" occurs and systems are developed without an understanding of how they contribute to broader national objectives.

STRATEGIC DOCTRINE AND C^3I OBJECTIVES

Since C^3I systems support the operations of our nuclear forces, the ways in which we plan to use these forces has an important impact on the specific functions that these systems should be designed to perform. Strategic doctrine provides general guidance with regards to the capabilities military forces should have, and how they might be employed in event of hostilities.

One of the critical aspects of strategic doctrine that affects C^3I requirements, and in turn is affected by C^3I capabilities, concerns the way we shall respond to a Soviet nuclear attack. In 1954 then Secretary of State John Foster Dulles articulated the concept of "massive retaliation." This doctrine stipulated that the United States reserved the right to respond to Soviet aggression anywhere in the world with a massive nuclear attack.[4] Since, in essence, we were threatening a "first strike" against the Soviets, the requirements on C^3I systems were not very great. If we were attacking first, the requirements for speed and survivability of C^3I systems would not be great; and since the attack was designed, in theory, to be one of attempted extermination, the President could make a "go" or "no-go" decision.

The viability of a doctrine of massive retaliation was questioned immediately, but it was not until 1962 that Secretary of Defense McNamara formalized an alternative to the Dulles concept. The new doctrine was based on the concepts of "flexible response" and "counterforce targeting."

Rather than responding to any aggression with a nuclear attack, the United States would use nuclear retaliation only in event of a Soviet nuclear attack; and rather than attacking cities, the United States would focus on destroying Soviet forces while retaining a secure counter-city capability.[5] Such a doctrine placed much greater burdens on C^3I systems since it implied that our forces needed to be able to absorb an enemy attack and then be prepared to execute a variety of options. The lack of enduring C^3I systems with capacity enough to handle more sophisticated traffic would require the President to make a decision in the few minutes between warning of an attack and impact of enemy missiles or risk of having any response neutralized. (Such a situation would have major implications for reliability and speed of warning systems.)

A major goal of U.S. strategic doctrine in the nuclear age has been to prevent a Soviet attack on the U.S. or its allies. "Deterrence" rather than victory has been our primary objective. A useful definition of deterrence can be found in the works of Thomas Schelling, a noted strategist. He states that deterrence is "the exploitation of potential force. It is concerned with persuading a potential enemy that he should in his own interest avoid certain courses of activity."[6] In other words, the threat of action is used to forestall the need to actually take action. Since deterrence involves threats, a major concern arises over the credibility of these threats. In order for deterrence to be credible, or believable, two objectives need to be met. In order for an enemy to be "deterred" he must be persuaded that first, we are capable of carrying out our threats, and second, that we are willing to do so. It is not necessary that the enemy be sure we meet both these requirements; the

fact that he can't be sure that we don't may be enough. The question of uncertainty is an important one. Though deterrence can be successful merely by making the enemy uncertain as to our capability and willingness to respond is a manner that will prevent his success, the critical problem is to determine what degree of uncertainty is needed to make deterrence credible.

Secretary of Defense Harold Brown articulated the requirements for deterrence and outlined a "countervailing strategy" designed to meet these requirements in his annual report to the Congress for fiscal year 1981. He said,

> For deterrence to operate successfully, our potential adversaries must be convinced that we possess sufficient military force so that if they were to start a course of action which could lead to war, they would be frustrated in their effort to achieve their objective or suffer so much damage that they would gain nothing by their action. Put differently, we must have forces and plans for the use of our strategic nuclear forces such that in considering aggression against our interests, our adversary would recognize that no plausible outcome would represent a success--on any rational definition of success. The prospect of such a failure would then deter an adversary's attack on the United States or our vital interests. The preparation of forces and plans to create such a prospect has come to be referred to as a 'countervailing strategy.'[7]

The doctrine expressed by Secretary Brown is not new. Like the policies of previous administrations, it has as its foundation the concept of "assured destruction." The primary objective of assured destruction is to deter a Soviet nuclear attack by insuring that the United States retains sufficient retaliatory capabilities after a surprise "worst case" Soviet nuclear attack, to cause "unacceptable" damage to the cities and industries of the Soviet Union. Just what is considered "unacceptable"

damage is another area of uncertainty, and the level of damage we must be able to inflict on the enemy has been debated over the years with no really accurate way to measure it.

In addition to the difficulties of measuring the adequacy of assured destruction, a strategy that limited to a massive countervalue response may not be sufficient. As Secretary Brown stated,

> Under many circumstances large-scale countervalue attacks may not be appropriate--nor will their prospect always be sufficiently credible--to deter the full range of actions we seek to prevent...the United States must be able to respond at a level appropriate to the type and scale of a Soviet attack. Our goal is to make a Soviet victory as improbable (seen through Soviet eyes) as we can make it, over the broadest plausible range of scenarios. We must therefore have plans for attacks which pose a more credible threat than an all-out attack on Soviet industry and cities...In other words, we must be able to deter Soviet attacks of less than all-out scale by making it clear to the Kremlin that, after such an attack, we would not be forced to the stark choice of either making no effective military response or totally destroying the Soviet Union. We could instead attack, in a selective and measured way, a range of military, industrial, and political control targets, while retaining an assured destruction capacity in reserve.[8]

The countervailing strategy as outlined above imposes certain requirements on our nuclear forces and hence the C^3I systems that support them. President Carter formalized the objectives that needed to be met in Presidential Directive 18. These objectives include:

- To secure a level of national entity survival at least as high as the Soviet Union;
- To assure the survival and functioning of a competent and credible National Command Authority, with minimum warning at all levels of nuclear attack;
- To assure the survival of a secure reserve force;
- To provide for the control of our nuclear forces throughout the course of a nuclear conflict.[9]

Various terms have been used to describe U.S. strategic doctrine, implying major changes in U.S. policy, such as "Assured Destruction" and "Selective Response." Ever since McNamara articulated the idea of counterforce targeting and flexible response, however, C^3I needs have been driven by objectives similar to those stated above. These objectives have called for C^3I systems that will enable the National Command Authority (i.e., the President or his authorized successors) to exercise deliberate and flexible choice before, during, and after an enemy nuclear attack.[10]

The objectives outlined in Presidential Directive 18 provide the basis for determining what the capabilities and functions of our forces should be which in turn serve as the basis for determining the general functional requirements for C^3I programs. C^3I requirements do not exist in a vacuum. These systems are only important in that they enable the forces to accomplish their objectives. Force objectives must be examined in order to determine what C^3I functions are needed, and these functions must be compatible with those objectives to be effective. Development of communications system, for example, should not begin with the question, "What is needed to enable the President to communicate with the nuclear forces after a nuclear attack?" Instead, the question should be: "What must our nuclear forces be capable of doing after absorbing a nuclear attack?"

The policy objectives outlined above are very broad, and this can cause problems. Before being useful, these broad objectives must be transformed into more specific requirements. When this is done, it is important to insure that the specific requirement agrees with the original objective. This seems obvious, but problems still occur and it is useful

to challenge these requirements. An example of this problem can be seen with regard to communications with submarines carrying ballistic missiles.

One of the objectives cited above is to provide for the control of our nuclear forces throughout the course of a nuclear conflict. This objective was transformed into a requirement: "In order to maintain a condition of readiness capable of carrying out a nuclear strike order from the National Command Authority, SSBN's [missile submarines] must remain in continuous communications reception."[11] Before one can say that the requirement is consistent with the objective he might ask, "Do all the SSBN's have to be capable of launching their missiles immediately?" It is not clear that the objective demands this but it is implied in the requirement.

CIVILIAN CONTROL OF THE MILITARY AND CENTRALIZATION OF AUTHORITY

Civilian Control

Just as strategic doctrine affects C^3I requirements, so too does the desire of the American people for strong civilian control of the military. Answers to the question of who should decide on the use of nuclear weapons play a major role in determining how our forces are controlled and what our C^3I needs are. The desire to insure civilian control over the military forces of the nation have determined to a large degree the command structure which controls the nation's nuclear forces (as well as all other military forces).

Manifestations of desire for civilian control over the military go back to the constitution itself. Article II, Section 2 states, "The President shall be Commander-in-Chief of the Army and Navy of the United States...." Though the President is constrained by the fact that Congress has the authority "to declare war...raise and support Armies... [and] to provide and maintain a Navy...," the Constitution gives him full operational control over the military forces of the United States. These clauses in the Constitution reflect the concern our founding fathers had about the potential inherent in military forces to overthrow the legally constituted government. As one scholar put it, "Society faces the danger that these forces of arms and the men trained in their use will be used against the society that trained them."[12] Though this has never occurred in the United States there are numerous

examples of such attempts elsewhere to keep the concern alive.

While the Constitution gives the President clear authority, the degree to which presidents have exerted control over the military has been influenced by three major considerations:

- The extent to which the survival of the nation is threatened
- Demands of domestic wartime politics and Presidential vulnerability to these demands;
- Command, control, and communications capabilities.[13]

Examples of direct presidential involvement in military operations are numerous throughout our history. George Washington took direct command of the Army in the field during the Whiskey Rebellion. President Madison personally directed the defense of Washington, D.C. during the War of 1812. President Lincoln was very active in the Eastern theater during the Civil War. In each of these cases the situation was a direct threat to the nation and the political survival of the President, and the theater of operations was small enough to exert personal control. Lincoln did not exert as much control over operations in the West due to C^3 limitations and the fact that operations there did not pose an immediate threat to the nation (in the East the Confederates threatened the capital).[14] In the Mexican War and the Spanish American War the United States was not threatened and communications to far-flung theaters of conflict was difficult, but both President Polk and President McKinley influenced the strategic conduct of the war for political purposes.[15]

In World War II communications capabilities were better, yet President Roosevelt's role in the direction of military operations was relatively limited for the following reasons:

- The United States was under no real threat of attack;
- F.D.R. was in his third term and was politically secure;
- He had faith in the military leaders he had chosen, and communicated well with them;
- He was deeply involved in coalition politics;

The widespread nature of operations made direct control difficult.[16]

The advent of the atomic bomb had a major impact on the role of the President as Commander-in-Chief. President Truman established the precedent of presidential control of nuclear weapons when he personally decided on the employment of the atomic bombs in 1945. This precedent was codified by the Atomic Energy Acts of 1946 and 1954 which state that only the President can authorize the use of nuclear weapons. The development of nuclear weapons greatly increased presidential involvement in military operations and their desire to centralize authority over military decisions. The United States was now in constant danger of direct attack and every crisis or conflict threatened the survival of the nation. Developments in the communications media, such as radio and television, brought crises directly into the living room of the American people as well as focusing attention on the President, causing him to feel political pressure to be personally involved in every

crisis. The same electronic revolution that affected the news media, however, also provided the President with the capability to communicate with military forces worldwide and provided the technology for the development of C^3I systems designed to increase his ability to directly influence all military operations.

The growing importance of tactical military decisions to larger national interests affected the degree of freedom local commanders are allowed to have. When national leaders were unable to affect local decisions due to constraints of communications technology, they had no choice but to delegate authority for tactical decisions to the local commander. Since the advent of atomic weapons, superpower confrontation, and worldwide communications, the stakes involved in tactical situations have risen, as has the capability of national leaders to intervene directly. The actions of a ship commander could now cause a major confrontation between nations (e.g., stopping Soviet ships during the Cuban Blockade) and seemingly minor operations were perceived to have potentially major consequences (e.g., cutting a tree at Panmunjoun). As a result, the presidents took a more active and direct role in tactical military operations (e.g., President Johnson in Vietnam, and President Ford in Mayequez incident).

Problems of national security, especially in current times, involve complex political, economic, social, and diplomatic issues all of which must be considered when making decisions. For a variety of social, political, and historical reasons, military leaders often do not take a very broad view, focusing instead on military factors. This is not

necessarily wrong, but in a complex situation, when terms like "victory" are not clearly defined, lack of a broad perspective can cause problems. While both F.D.R. and Eisenhower had a great deal of faith in their military advisors (and as a result the advisors played a more central role in decisions), Kennedy's experience was not as favorable.[17] After the Bay of Pigs he made it quite clear that he wanted military operations under ultimate civilian control when he said in a statement on national security policy in 1961:

> We propose to see to it...that our military forces operate at all times under continuous, responsible, command and control from the national authorities all the way downward--and we mean to see that this control is exercised before, during, and after any initiation of hostilities...[18]

President Kennedy's faith in the ability of his military leaders to consider non-military factors was further shaken during the Cuban missile crisis. Robert Kennedy recounted the inability of the Joint Chiefs of Staff (JCS) to look beyond the limited military concerns during the crisis, in his book The Thirteen Days. According to him, President Kennedy was disturbed by their limited perspective, as exemplified by one military leader's desire to use nuclear weapons in an attack on Cuba, on the basis that in such a situation the Soviets would do so.[19]

All of these concerns are magnified a thousandfold with regard to controlling the release of nuclear weapons. As stated earlier, the President is the sole authority for releasing these weapons. The desire to insure that he is capable of exercising that authority when needed as well as a desire to prevent unauthorized release have been major factors

promoting the centralization of authority and the organization of the national military command structure.

The National Military Command Structure

The modern national command structure stems from the National Security Act of 1947 and subsequent amendments. This act established the National Security Council, the Central Intelligence Agency (CIA), and most importantly, a "unified" military establishment headed by the secretary of defense. In this act, the secretary of defense was designated as "the principal assistant to the President in all matters relating to national security." He was given authority to "establish general policies and programs for the National Military Establishment," and, "exercise general direction, authority and control over such departments and agencies." This was amended in 1949 to read, "The Secretary of Defense shall be the principal assistant to the President in all matters related to the Department of Defense. Under direction of the President, and subject to the provisions of this Act, he shall have direction, authority and control over the Department of Defense."[20]

The role of the secretary of defense is an important one, and can be directly related to the increased political demands that threats to the national security place on the President. He has grown to be one of the most important political appointees in the nation. Being a political appointee of the President, the secretary can be expected to recognize and react to the political demands placed on the President by the threat of nuclear war and the dangers of crisis situations. Also, being an appointee, the President can remove him if he fails to maintain the

President's perspective. Given these ties, a strong secretary of defense provides the President with much better control over the complex issues of national security, and with the assistance of the broad powers provided by statutes, the two men can exercise close control over the military forces of this nation. To further cement the close teamwork of the President and the secretary, and to codify their preeminence over national security, Department of Defense (DOD) Directive 5100.30, was published in 1971, and defined the National Command Authority (NCA) as consisting only of the President, the secretary of defense, or their duly deputized alternates or successors.[21]

The Act of 1947 gave the secretary of defense the authority to establish the rest of the chain of command within the department with some statutory restrictions. It also gave the secretary the authority to "exercise any of his powers through, or with the aid of, such persons in, or organization of, the Department of Defense" as long as such action was not "specifically prohibited by law."[22] In 1958, however, a Reorganization Act further specified authority within the Department of Defense. It authorized the President, through the secretary of defense, with the advice of the Joint Chiefs of Staff, to establish unified and specified commands for the performance of military missions. It further stated that "such combatant commands are responsible to the President and the Secretary of Defense for such military missions as may be assigned them by the Secretary of Defense, with the approval of the President," and that the commanders of unified and specified commands would exercise operational control over all forces assigned to them rather than the individual military services.[23] These commands included those responsible

for strategic nuclear weapons (e.g., Strategic Air Command [SAC]).

It is important to note that the role of the Joint Chiefs of Staff in the chain of command is greatly restricted, and that the military departments are not in the chain of command. When Congress established the Department of Defense it made clear its intent to retain separate military departments and "to provide for their unified direction under civilian control of the Secretary of Defense but not to merge these departments or services...to provide for the unified strategic direction of the combatant forces, for their operation under unified command...but not to establish a single Chief of Staff over the armed forces nor an overall armed forces general staff."[24]

The limitations on the role of the Joint Chiefs of Staff are clearly spelled out in legislation. The JCS are authorized to prepare strategic plans and provide for the strategic direction of the armed forces, as well as perform a variety of other staff functions for the secretary. They are given the authority to "perform such other duties as the President or Secretary of Defense may prescribe."[25] While this allows them a place in the chain of command, the statute cited earlier makes it clear that they are not intended to have a discretionary or operational command authority. The fact that unified and specified commanders are responsible directly to the secretary of defense also limits the statutory authority of the JCS. The intent of Congress to restrict the JCS to mainly a staff role under the direction of the secretary of defense is further demonstrated by the designation of the chairman as the ranking military officer yet stating that "he may not exercise military command over the Joint Chiefs of Staff or any of the armed forces." The statutes also specifies that

the joint staff "shall have no executive authority."[26]

The result of these prescriptions is that the JCS have no independent authority but that the secretary may give orders through the JCS, and they may direct the actions of the unified and specified commanders under a delegation of authority from the secretary. This role of the JCS is further delineated by DOD directives (JCS Publication 2) which gives the JCS the responsibility "to provide guidance and direction to the commanders of unified and specified commands on all aspects of command and control which relate to the conduct of operations in accordance with pertinent DOD instructions.[27]

Though each service secretary is responsible for, and has the authority to conduct all affairs of his departments, and the respective chiefs of staff are authorized "to exercise supervision over such of the members and organizations...as the Secretary [of the Department] determines," the statutes state that such authority and supervision exercised in a manner consistant with the full operational command vested in unified or specified commanders...."[28]

The chain of command as established by legislation and promulgated by DOD directive specifies the chain of command to be from the President to the secretary of defense, through the JCS to the unified and specified commanders and down to their subordinate component commanders. It is important to note, however, that the chain of command does not coincide with the communications chain. DOD Directive 5100.30 states that the channel of communication for execution of the SIOP is from the President to secretary of defense (the National Command Authority [NCA]) through the chairman of the JCS directly to the executing commanders. Executing

commanders are those who directly control nuclear weapons. This chain of communications bypasses the unified and specified commanders, and could bypass all levels between the chairman and the captain of a missile submarine, or an ICBM squadron. With the current communications capabilities available to the President it is possible for the NCA to bypass the entire military chain of command (as has been done in periods of crisis). This is not prohibited by statute, since the secretary is authorized to exercise his power as he sees fit.

Centralization of Authority

The national command structure provides the potential for a great deal of centralization of authority, as do advances in communications technology that enable the National Command Authority to bypass the chain of command and deal directly with forces executing a military mission. There are some problems that occur as the result of centralization that should be considered, however. The ability of the President to bypass the military chain of command may increase his control and insure operations are properly conducted, but it can cause a deterioration in the ability of subordinates to act independently should the need arise. The overriding of local authority by higher level decision makers cause frustration in those bypassed, especially if they feel they have retained the responsibility for the operations, while losing authority over them. Even if this is not a problem, middle-managers' ability to deal with problems independently could deteriorate as they will get used to "passing the buck."

Currently, the President gets directly involved in relatively small

military operations. Should a major war break out, with many operations being conducted simultaneously, he could no longer deal with them all. If his subordinates are not trained and experienced at making independent judgments, then there could be problems.

Centralization also places a heavy burden on C^3 systems. Should communications fail due to enemy interference, centralization could result in lack of flexibility at lower echelons, and even paralysis, as commanders wait for orders from above. Though the problem does not in itself justify decentralization in light of the other issues, effort should be taken to insure that the chain of command plays an active role and is kept informed (e.g., by crisis conferencing).

Another concern with regard to centralization is the adequacy of the C^3I systems to meet the needs of centralized control. The ability of C^3I systems to communicate and process information are important factors affecting centralization. Communications limitations affect the quantity and timeliness of information. If information arrives too late, or in insufficient quantity, then the central authority cannot make an informed decision and he will have to delegate authority to the local level where the necessary information can be obtained more quickly. Though decision makers often complain about lack of information, too much raw information can be a problem also. Volumes of raw, unstructured information (often referred to as "data") is of limited use to decision makers. What he/she needs is relevant information that has structure, form, and organization. Since information processing utilizes valuable resources, issues such as how much and what kind of information will assist the decision maker, must be answered. There are trade-offs between the need for "filters"

in the system to eliminate irrelevant data and to check accuracy of information, and insuring rapid transmission of information to the decision maker.

If the President wants a system that is responsive to his requirements, he must be sure to give specific guidance and participate in its development. Otherwise military planners design the best system possible from their viewpoint, only to find it does not meet the needs of the NCA; then he has to resort to ad hoc procedures, which bypass the filtering process and result in data overloads at the top. C^3I systems are only effective if the requirements they must meet are clearly specified. Once this is done the system can be designed to satisfy these requirements more effectively.

THE SOVIET THREAT TO C^3I

An understanding of the threat from Soviet military capabilities that C^3I systems face is important in determining requirements for particular systems. Therefore it is useful to review the dimensions of the threat that these and other capabilities pose to our C^3I systems. The major areas of concern are the following:

- Physical destruction of facilities by nuclear blast or conventional attack;
- Electro-Magnetic Pulse;
- Electronic Interference due to Nuclear Detonation;
- Electronic Counter-Measures (ECM);
- Sabotage;
- Anti-Satellite Weapons (ASAT).

Physical Destruction

Overt physical destruction of our C^3I facilities is a major threat in a nuclear war. The Soviets can use either conventional or nuclear weapons to attack command centers, communications sites, etc. Increases in the size of Soviet nuclear forces over the last twenty years changed the threat to C^3I systems.

In order to meet the Soviet nuclear threat in the era of massive retaliation, C^3I systems were developed to warn of an attack by Soviet bombers and to direct air defense efforts. The construction of the "DEW Line" early warning radars, the SAGE air defense system, and the deployment of interceptors, gave considerable confidence that the effects of an attack could be minimized and our retaliatory forces protected. Because of the relatively small number of weapons available and poor delivery accuracy, C^3 systems were not seriously threatened. Command centers and critical communications links could be, and were, protected by "hardening" and dispersal outside cities, which were considered the primary targets of a nuclear attack. Since bombers were the sole means of delivery of nuclear weapons, there were several hours of warning available for leaders to be evacuated, bombers to be alerted, and decisions concerning response made.

During the 1960's the strategic environment changed dramatically. The numbers of weapons greatly increased; ICBM's that could reach targets in as little as thirty minutes were deployed. In the early 1970's Soviet deployment of MIRV's greatly increased the number of warheads that could be delivered. Warhead accuracies also improved, thus decreasing the ability of hardened targets, such as command centers, to survive a direct attack.

As a result of these changes, the burden on C^3I increased. The reduction in weapons' delivery time necessitated a more rapid and effective warning system. Command and control centers and communications systems were becoming vulnerable due to the increase in the numbers and accuracy of warheads. The endurance required by current strategic doctrine has become much more difficult to achieve. Though our nuclear forces are designed to be able to "ride-out" an attack, maintaining effective command and control over them has become much more difficult.

A study for the Department of Defense by the Stanford Research Institute in 1962 pointed out the lack of endurance inherent in our C^3I system at that time.[29] Since then, the threat has greatly increased while some of the problems pointed out in the 1962 study remain.

The major effects of nuclear weapons that could cause physical destruction of C^3I facilities are the following:

Blast;

Thermal effects;

Radiation.

These destructive effects of nuclear weapons, though of greater magnitude than those of conventional weapons, are still essentially local in nature. That is why the increase in the quantity and accuracy of Soviet warheads is so important. The large number of warheads that the Soviets can target on C^3I facilities make survivability an important consideration.

Electro-Magnetic Pulse

One of the effects of a nuclear explosion that is particularly threatening to C^3I systems is called Electro-Magnetic Pulse (EMP). This

phenomenon is of interest because it can severely affect communications systems and computers. It can cause temporary blackouts of communications and radar, upset electronic circuits, and damage sensitive electronic equipment.

EMP is a prompt effect of a nuclear explosion which results from the interaction of gamma rays released by the detonation, and air molecules. Electrons are stripped away from the air molecule, which causes a current flow which can radiate electromagnetic energy. EMP in itself is not harmful but once collected by metallic conductors it can cause tremendous voltage and current surges, similar to lightning. Like other radiation, EMP from a low-level burst is attenuated by the atmosphere and is not militarily significant at ranges much greater than other weapons effects (e.g., 15 km. for a 40 kt. surface burst); however, when a nuclear weapon is exploded outside the atmosphere a much larger effect occurs. A very small number of exo-atmospheric bursts (300-500 km. high) can generate EMP of sufficient intensity to damage unprotected electronic equipment, computers, and communications equipment throughout the United States.[30]

EMP effects are of two main types: functional damage and operational upset. The former is a permanent failure such as burned out transistors or blown fuses, while the latter refers to a temporary disruption of a system, such as activation of electronic relays.

The importance of EMP was not widely recognized until 1960, when concern began to mount over the vulnerability of electronic systems. The signing of the Nuclear Test Ban Treaty prevented extensive testing of EMP effects and today there is some uncertainty and debate regarding

the extent of the threat posed by EMP.[31]

Ironically, advances in computers, electronics, and communications equipment have resulted in increased vulnerability to EMP. Transistors and solid state circuitry are much more vulnerable than vacuum tubes were.[32] Most susceptible are high speed computers, especially those employing transistors or semiconductor rectifers (which most computers now use). Power transmission equipment and transistorized telephone switching equipment are also vulnerable. Almost all unprotected communications equipment is vulnerable, due to the broad frequency range of EMP, especially very high frequency (VHF) and ultra high frequency (UHF) radios systems. Antennas provide sufficient EMP field generation to burn out unprotected radio components.[33]

Though most communications and electronic equipment is protected against lightning, which also produces intense electrical surges, the faster "rise time" (time to reach peak voltage) of EMP makes much of the conventional lightning protection ineffective. There is considerable controversy over this issue, and with limited ability to gather empirical data, the debate is not easily resolved.[34] Recent government studies indicate however that, though lightning protection efforts are helpful, many fall short of offering assured protection against EMP. Technology for EMP protection is advancing and C^3I systems can be safeguarded, though it can be an expensive proposition. It is less expensive to design EMP protection into new equipment than it is to retrofit existing systems. This is an important consideration when contemplating system development. It also impacts significantly on any plans to utilize commercial telecommunications networks for C^3I purposes as the plant in place lacks

protection to a large degree.

Satellites are also vulnerable to EMP. The widespread use of weight-saving advanced electronics technology in satellites makes them especially vulnerable to nuclear blasts hundreds of kilometers away, if not protected. The type of protection needed is more complex and difficult, since normal methods of shielding electronic equipment are too heavy for use on satellites.[35]

The Nuclear Test Ban Treaty has limited the ability to verify the extent of the threat posed by EMP. This may be a blessing in that it creates uncertainty in the minds of the Soviets as to what the effects might be. It is difficult to tell how much they know about EMP, however, so it seems unwise to dismiss what could be a very potent threat. The problem that has to be confronted again and again is, if protection is expensive, "how much do we spend to protect systems from an uncertain threat?"

Electronic Interference

In addition to the direct effects of EMP, high altitude nuclear bursts can cause extensive disruptions in the atmosphere that affect radio communication. Exo-atmospheric detonations can cause radio disruptions across the entire frequency spectrum, from ELF to SHF. The duration of the disruption ranges from minutes for SHF, to hours for VLF, and extends over thousands of square kilometers. In addition to temporarily "blacking out" communications, the blasts can cause the ionization of regions of the ionosphere hundreds kilometers in diameter, lasting several hours. This disruption would not necessarily prevent communications, but could degrade

them and cause errors in digital signals.[36]

The effect of numerous nuclear detonations both inside and outside the atmosphere cannot be precisely determined. The implications of this uncertainty are both positive and negative. On the plus side, an attacker may hesitate to use extensive exo-atmospheric explosions for fear of disrupting his own C^3I. On the negative side, the cumulative effects of many explosions could overstress our telecommunications, electronics, and power systems to such a degree that there will be widespread comprehensive failure, leaving the nation's nervous system essentially paralyzed.

Electronic Counter-Measures

Electronic counter-measures pose a special threat to surveillance and communications systems. ECM could neutralize these systems without destroying them physically. The ECM threat consists mainly of "jamming" and "spoofing." Jamming involves the disruption of communications and warning systems by preventing them from receiving coherent signals. Spoofing is more subtle and involves the introduction of false messages into the C^3I system. Both can hamper our ability to gather information and transmit it.

Jamming is created by sending strong signals to a receiver that prevents it from receiving signals from other sources. The effectiveness of jamming depends on the ability of the jammer to locate the frequency that the enemy emitter or receiver operates on and sending a more powerful signal on that band than can enemy stations, or such that the receiver is overloaded. Jamming is a double-edged sword, however, since friendly forces cannot use a frequency that is being jammed either.

Spoofing is designed to mislead the opponent, by causing false signals to be received. The transmission of false signals and messages can confuse surveillance efforts and lead to disruption in controlling forces. There does not seem to be a large role for spoofing with regard to warning systems, with the exception of attempts to electronically camouflage activities. It is possible that, by causing U.S. warning systems to receive false signals indicating a nuclear attack, the Soviets could reduce the credibility of these systems and create a delay in U.S. response to an attack. This would be a high risk strategy, however, since in spite of our public statements they could not be sure that we might be convinced that they were really attacking us and retaliate.

Sabotage

In an open society with few restrictions on access, the threat of sabotage to critical C^3I facilities cannot be ruled out completely. While a nuclear attack on warning systems or communications facilities would likely result in some sort of nuclear retaliation, a clandestine attack on these same facilities, while causing alarm, would be less likely to result in a nuclear response. This is especially true if the saboteurs claimed to be domestic dissidents (e.g., a group protesting the environmental impact of microwave emissions from PAVEPAWS warning radars--a recent controversy).

Anti-Satellite Threat

Communications and surveillance satellites are vulnerable to enemy anti-satellite (ASAT) efforts as well as EMP. The ASAT threat is developing as a result of Soviet testing of an ASAT system. During the period

between 1967 and 1970, they demonstrated that they were able to launch a manueverable satellite to rendezvous with one already in orbit. Though no target satellite was known to have been destroyed, the ability to rendezvous overcame a major obstacle to destroying a satellite.

In 1976 the Soviets launched several satellites which intercepted satellites in orbit. Some of the interceptor satellites were observed to explode in the vicinity of the target representing a further development of a viable ASAT capability that does not involve the use of a nuclear weapon.[37]

It is difficult to protect satellites against attack since hardening would add excessive weight and would need to be extensive to protect against even a non-nuclear attack. It may be possible to develop defensive systems to protect our satellites ("Anti-ASAT's") which conjures up visions of a war in space. Another approach would be to "hide" additional satellites in high orbits that could be activated should be to "hide" additional satellites in high orbits that could be activated should operational ones be destroyed or damaged. It takes several hours for an ASAT to climb within reach of a platform in synchronous orbit so potential attacks could be detected in time to prepare a dormant satellite and it would be saved from attack for a period of time. Proliferation of the number of satellites would make their destruction very difficult and provides another option to increase survivability.

ASAT programs are not limited to destruction by interceptors. There is evidence that the Soviets are working on ground-based systems designed to "blind" our infrared surveillance satellites with laser beams. Though there appears to be no evidence that their efforts to develop such systems have been successful, this may become a threat at some future date.

C^3I FUNCTIONAL REQUIREMENTS

The strategic policy objectives outlined by President Carter require that the U.S. be prepared to fight a protracted nuclear war, if necessary. In order to be able to support the conduct of such a war (and thereby hopefully prevent it) C^3I systems need to be able to perform several functions:

- Provide timely warning of a nuclear attack;
- Provide accurate attack assessment;
- Provide for the survival of the National Command Authority;
- Communicate from the NCA to the nuclear forces;
- Monitor execution of decisions and assess results;
- Provide for the re-constitution and re-direction of surviving nuclear forces;
- Enable nuclear operations to be terminated at the command of the NCA as well as assisting in termination of conflict.[38]

Though these requirements are still quite broad, an examination of each can help identify important considerations that should be addressed when developing specific requirements for particular systems, as well as when evaluating current and proposed capabilities.

Provide Timely Warning of a Nuclear Attack

Wallace Henderson, director for indications and warning in the office of the assistant secretary of defense (C^3I), stated in 1978, "Given that the probability is high that we will ignore the information assembled from our national/technical intelligence sources which indicates that the other side really intends to go to war, tactical warning needs

to be highly credible to overcome the mind set that says, 'It cannot really happen, we've got it all under control in the political environment.' To be highly credible, tactical warning must answer WHAT is it, WHO did it, are we the SUBJECT of the attack, WHEN was it initiated and, of course, WHEN will it arrive."[39] In order for the warning to be credible the questions raised by Mr. Henderson need to be answered accurately, as a result, elimination of errors is a key goal.

Errors in warning systems are basically two types: "false negatives" or "false positives." A false negative is the failure to detect a launch when one occurs. This is the most serious error, as it would lead to the absence of any warning of an attack. Such an error could be caused by equipment malfunction or enemy electronic counter-measures (ECM), such as jamming or blinding sensors. In the latter case, we would know something had happened but would not know what it was.

A false positive, which is the detecting of a launch when one does not occur, could be almost as serious. The danger is that we might launch a counterattack based on a false alarm. One of the ways to avoid this type of error is to allow the enemy warheads to impact so that there is no doubt that an attack has occurred. False positive can be caused by, equipment failure, natural phenomena, or enemy ECM (called "spoofing").[40]

In order to reduce the possibility of error, warning systems can be, and are, made redundant, and can utilize "dual phenomenology." The concept of dual phenomenology essentially entails the use of different types of sensors to back each other up. For example, infrared sensors could be used to detect ICBM launches, but radar systems would also be employed to verify the launch. Redundancy would ensure that the elimination

of a warning site would not create a hole in surveillance coverage. A variety of warning systems is also needed due to the fact that the Soviets can use ICBM's, SLBM's and bombers. Whereas high level radar and satellite-based infrared detection could warn us of a missile attack, low flying bombers would not be detected without a low level radar that, in turn, would be of little use in detecting missiles.

Because of the short flight time of enemy missiles, responsiveness is an essential element of warning systems. Currently, it takes approximately 30 minutes for a Soviet ICBM to travel from its launch fields to the Minuteman bases in the U.S.; it could take as few as five to ten minutes for a missile from a Soviet submarine lying off our coast to hit Washington, D.C.[41] Given these short time spans, surveillance systems must not only detect an attack quickly, the information must be disseminated rapidly and assessed without delay. Only "real-time" or "near real-time" information will be useful.

The issue of survivability is also an important one. Destruction of warning systems would "blind" our decision makers; and, while providing "strategic" warning of a possible attack, they would prevent any tactical warning from being given. Some would argue that for this reason it would be foolish for an attacker to destroy warning systems because the opponent, once blinded, would have an incentive to escalate to a general strike. The problem with this view is that it assumes a president would condemn over 140 million Americans to death for a few warning sites because there was a chance of an enemy attack. It should also be noted that nuclear weapons are not needed to destroy radar sites, so the United States could be blinded without the provocation of a nuclear attack.[42]

Provide Accurate Attack Assessment

Attack assessment has two major aspects. The first is to determine the type of attack before impact (a function of the warning system). It would be very difficult to completely characterize an attack before impact, however. The surveillance systems will not be able to distinguish decoys from real warheads very accurately, nor will precise information about yields or detonation strategy (e.g., use of ground bursts to increase fallout) be available. However, an initial assessment of the type of attack can provide a limited opportunity to take action to protect our nuclear forces, as our land-based missiles become more vulnerable and the President must decide to "use them or lose them." If we were to adopt a "Launch on Warning" policy, this type of assessment would be of extreme importance in order to decide on an appropriate response. However, since our forces are designed to absorb an enemy attack, the need for pre-impact attack assessment is reduced, and post-impact attack assessment assumes a position of primary importance.[43]

The following types of information are needed as part of the post-impact attack assessment:

- Extent of damage to the civilian sector of the nation and casualty estimates;
- Extent of damage to U.S. nuclear forces and operational status of surviving forces;
- Post-attack status of Soviet nuclear forces;
- Knowledge of enemy military activity world-wide;
- Knowledge of military and diplomatic activities of allies and neutrals.

If the President is to have the option to use a selective response in the hopes of controlling escalation, he must have rapid access to information concerning what kind of attack the enemy has launched. Obviously, if we cannot tell the difference between a counterforce or countercity attack, then escalation control is hopeless. In order for an effective targeting strategy to be carried out the NCA must know what U.S. forces have survived and what their capabilities are for action. Knowledge that significant numbers of ICBM's with a hard target capability are available may permit him to pursue options that would be precluded without such forces. For example, he could decide to retaliate against the enemy's strategic reserve in an attempt to limit further damage from additional enemy strikes. Such a decision also requires knowledge as to which forces the Soviets used in their initial attacks in order to avoid wasting weapons from an already reduced arsenal (in the case of an enemy counterforce attack) on empty silos.

The information requirements discussed here require a much more complex information system than would be needed solely for assured destruction. If that were our only objective then the only information requirement would be a knowledge that an attack has occurred. The objectives of the countervailing strategy require that communications systems be able to handle large volumes of data in a highly stressed environment, and therefore, these systems need to be configured so that connectivity would be retained throughout an attack or could be rapidly re-established after an attack. The need for reports on the status of friendly forces puts an additional burden on the communications/information system. Rather than a one-way, low-capacity system from the NCA to the forces, a two-way,

high-capacity system is needed to transmit orders downwards and information upwards, and to process that information.

The rapidity with which this information can be assimilated will affect the efficacy of our response. Should delay be too long the enemy may have time to assess his own attack and strike again, or take action to reduce the effectiveness of any U.S. countermeasures, by relocating key personnel, dispersing forces, or moving weapons (such as re-loads for used silos). The accuracy of the information is also important if the President is to avoid wasting limited retaliatory forces. Since accuracy often is gained at the expense of speed these are trade-offs that must be considered.

Survival of the National Command Authority (NCA)

The National Command Authority refers to those persons authorized to make the decision to use nuclear weapons. As was stated earlier, the sole power to make this decision rests with the President or his authorized successor. As a result, the survival of someone authorized to decide what response to make to an attack is an important factor. It should be noted that though it is preferable for the President to survive, it is not essential, and given his high visibility, it may be a goal that is difficult to achieve should the attacker wish to "decapitate" our command structure. The enemy's hope in such a situation would be that in a highly centralized system, as is our command structure for nuclear release, the elimination of the decision maker could paralyze any response.

The survival of the President may be very difficult to guarantee. For this reason it is important to have effective procedures for passing

control of the nuclear forces to a duly authorized successor and insuring that a successor is able to make an intelligent decision concerning a U.S. response. It is important to note that while we may think of an individual as being able to give the orders to launch nuclear weapons, he requires an organization to support him. The survival of the individual without the organization may well be useless, so some means of insuring the survivability of national command center is needed. The size of the command group depends on the complexity of the decisions being faced and the volume of data processed. ADP equipment is an essential element of such a center in light of the demands placed on it (or them). Prior knowledge of SIOP options and security issues will also be necessary if the successor is to make a timely response.

The concern about the possibility of the enemy paralyzing our ability to retaliate after an attack, by "decapitating" our command system, should not be dismissed lightly. However, the extent to which this is a threat is the subject of some debate. It could be argued that the enemy would have little interest in destroying the NCA because, with this leadership gone, terminating the war would be difficult. One method of promoting NCA survivability would be to create uncertainty as to the results of such an action. This could be done by insuring that the lack of an NCA does not physically prevent military commanders from launching their forces. If destruction of the president puts the decision to launch a nuclear retaliation in the hands of an Air Force general located in an airborne command post (whose family, living on an Air Force base, would most likely be dead), the Soviets may well make a concerted effort to insure that the civilian leadership survives and is able to control the

surviving nuclear forces.

The concern over "decapitation" points out the tension between a desire to limit the ability to launch nuclear weapons (in order to prevent accidental or unauthorized launches) and the danger of creating a small number of critical "nodes" in the control system, whose elimination would paralyze our forces. (This will be discussed in more detail in the section, Current C^3I Systems.)

One of the primary elements of American strategic doctrine discussed earlier is the capability of our nuclear forces to absorb a nuclear attack without losing the ability to retaliate effectively in a variety of ways. This objective requires the survival of the communications systems needed to provide direction to these forces. When developing systems to meet this requirement several questions should be considered, three of which are:

- Must communications be continuous? If not, how quickly must they be restored?
- What kind of communications capacity will be needed?
- How quickly must orders be transmitted?

Transmission of Orders to Nuclear Forces

The third major requirement for the communications systems supporting strategic command and control is the transmission of the national command authority's decision to the nuclear forces. This requirement has become more difficult because the number of Soviet warheads available for targetting our communications facilities increased, and greater traffic capacity is needed to transmit a wide variety of response options.

Monitor the Execution of Decisions

It is important that the NCA be able to monitor the execution of a decision to use (or not to use) nuclear weapons to respond to any enemy attack. Such monitoring would enable weapons to be re-programmed in case of malfunctions or misses, in order to insure target coverage. To be successful the NCA must have information about friendly forces and a means of assessing damage to the enemy caused by U.S. nuclear strikes. To get this information, communications systems must remain operative, and surveillance systems must also be available. Survivability and re-constitutability of our surveillance systems will be important if the NCA is to get intelligence on damage to the Soviets and their surviving forces. Satellites currently provide the most effective means of gathering information. If they are to provide intelligence after an attack, efforts to protect them from destruction by the enemy must be taken. The threats posed by EMP and the development of a Soviet ASAT capability require that consideration be given to increasing the survivability of both the space platforms and their communications links to the NCA. Other means of gaining intelligence include use of manned bombers to provide damage assessment while conducting their attacks, or by sending out reconnaissance aircraft or drones to provide needed information.

Reconstitution and Re-direction of Forces

In the event of a protracted nuclear war, there will be a need to manage the use of remaining nuclear forces and to insure that they are protected from further attack. This applies particularly to the submarine and bomber forces. Some of the objectives that C^3I systems will need to

be able to support include:

- Recovery of surviving bombers to surviving airfields, re-loading, and re-deployment for future operations;
- Re-supply and direction of SSBN's to include the possibility of re-loading them with new missiles;
- Re-targeting weapons as intelligence provides information on Soviet activities;

  Integration of nuclear operations with other worldwide operations.

These, and other objectives, require communications systems of much greater capacity than those required merely for the transmission of Emergency Action Messages (EAM). Flexibility and adaptability will also be important in view of the widespread destruction that can be expected to result from a nuclear attack.

Conflict Termination and Escalation Control

Inherent in the objectives articulated in PD-18, is the requirement to be able to end a nuclear conflict and control escalation in order to avoid mutual destruction. This goal was articulated as early as 1975 during the Ford administration by Secretary of Defense James Schlesinger who stated that the use of American strategic forces should "have prospects of terminating hostilities before general war breaks out, and leave some possibility of restoring deterrence."[44] Without some ability to terminate a conflict, there is little hope of preventing escalation, resulting in a continuance of destruction until both sides exhaust their arsenals, or their societies collapse.

Though many strategic thinkers, such as Herman Kahn, believe that any nuclear war will inevitably escalate to a massive nuclear exchange

destroying both parties, it seems useful to make every attempt to increase the possibility of limiting escalation in such a situation, should deterrence fail.[45] Secretary Brown articulated this view when he identified as one of the objectives of U.S. strategic policy, the need to "leave open the possibility of ending an exchange before the worst escalation and damage had occurred, even if avoiding escalation to mutual destruction is not likely."[46]

Others argue that the ability to control escalation, once nuclear weapons use had been initiated, would lower the "nuclear threshold" and could increase the likelihood of war occurring.[47] Such a fear is due to a concern that the Soviets might believe that they could initiate a war without suffering massive destruction. This concern does not take into account the issue of uncertainty, however. For the Soviets to risk a "limited" nuclear war, they would have to be reasonably certain that escalation could be controlled. The availability of options to control escalation does not mean they will be used or will be effective. The desire to increase the level of uncertainty may be a reason that public statements of leaders in both the United States and the Soviet Union emphasize that successful escalation control is doubtful. Though maintaining this uncertainty is useful, and prevention of escalation of mutual destruction may be unlikely, it seems unwise to prevent the President from having a choice in the matter.

One scenario for escalation control that is compatible with the countervailing strategy would be a "tit-for-tat" type of exchange. In such a scenario we would endeavor to insure that Soviet losses would neutralize whatever gains they hoped for from a limited attack on the United

States. Another scenario involves a counterforce response designed to limit future damage potential from additional Soviet attacks, but expressly avoiding cities or control mechanisms, the destruction of which could prevent war termination. These scenarios require sophisticated, survivable, command, control and communications; and according to Secretary Brown's testimony, we need such systems if "we are to respond appropriately to an enemy attack and have some chance of limiting the exchange."[48]

One of the major reasons for attempting to control escalation and fight a "limited" nuclear war is that such an approach may enable both sides to terminate the conflict other than by mutual destruction. However, if nuclear conflict is to be terminated short of mutual destruction, the concept of victory must be limited to an attempt to restore the status quo. Demands for unconditional surrender would most likely result in escalation, unless the opponent was disarmed.[49] The goal is to avoid putting the opponent into a position where he has nothing to lose.[50]

Such a concept requires that the command authority on both sides be able to communicate with, and control their respective forces, and that they be able to communicate with each other. It would therefore be counterproductive for either side to target the other's command-control-communications. Such a situation would seem to fit a scenario in which the attacker launched a limited nuclear strike, not in order to win a nuclear war, but in order to avoid losing a conventional conflict or some other confrontation. Concern about C^3 vulnerability would indeed seem less in this case.

We cannot ignore the fact that the Soviets do not consider nuclear wars unwinnable. A recent Defense Department study states, "It is

difficult to appreciate the sacrifices to which the Soviet leadership may be willing to submit the Russian population and economy in order to maintain the power of the CPSU. Victory in a nuclear war is the only outcome that makes the enormous sacrifices of a nuclear war worthwhile."[51] Soviet military writing also emphasizes that they can not only survive, but can also win a nuclear war.[52]

In light of these statements we cannot dismiss the idea that the Soviets might try and disarm the U.S. by attacking strategic forces and C^3. If we are to terminate the war without escalating it, we must not only be able to direct our forces to exercise controlled retaliation to prevent the Soviets from capitalizing on their attack. We must be able to re-establish deterrence and begin a dialogue aimed at cessation of hostilities.

QUALITIES NEEDED IN C^3I SYSTEMS

In order for C^3I systems to support effectively the objectives of United States strategic policy and perform the functions outlined in the previous section in the face of a growing Soviet threat, they must have several qualities. Systems planners attempt to maximize these qualities subject to technological limitations and resource constraints. These attributes are often in conflict with each other and are not absolute characteristics. Consideration of these qualities and the tensions that exist between them provide a means of determining system capabilities. The major qualities that shall be discussed in this paper are:

- Survivability;
- Credibility;
- Flexibility;
- Responsiveness;
- Security;
- Integration;
- Reliability.[53]

Survivability: Various Approaches

The capability of the United States to retaliate after a Soviet attack is affected by two major limitations: the survival of nuclear delivery vehicles and the survival of a command and control system capable of directing these forces. The problems of force survivability have received a great deal of attention without an enduring system for controlling these forces, however, they are useless. In fact, having surviving nuclear delivery systems without any control over them could be worse than useless,

as unauthorized use of these weapons could hamper efforts to terminate the conflict. Just as damage to the human nervous system can prevent healthy muscles from functioning, damage to the C^3I elements of our nuclear forces can prevent those forces from being used effectively. Bernard Brodie, one of America's foremost nuclear strategists, pointed out the importance of survivable C^3I saying, "It is also vital to remember that the defense of a retaliatory force capability is defense of a system, one which comprises not only the bombardment vehicles but also the relevant decision-making authority -- which begins with the commander-in-chief -- as well as the communications system by which the decision is translated into action. Enemy planners are bound to be constantly searching for the weakest link in our retaliatory system -- a 'go' or 'no-go' decision may very well be dominated by a developing conviction that it is possible to paralyze our response."[54] Dr. William Perry, under secretary of defense for research and engineering, also identified this problem, saying," We must assume that the Soviets would plan to attack those links whose loss would greatly reduce the effectiveness of our forces."[55] In order to ensure that our forces can be effectively used, the Defense Department has been concerned about the survivability of C^3I systems.

Survivability can be defined as "the ability to exist and function satisfactorily after, or in spite of, nuclear conflict, conventional conflict, sabotage, or natural disaster.[56] An important consideration to keep in mind is that when related to C^3I, survivability does not necessarily refer to specific facilities but rather to the maintenance of capabilities or functions. C^3I functions are performed by systems, rather than individual pieces of equipment. Many individual elements of a system

may be destroyed, yet the system "survives" if it can perform its functions with what remains.

A major way to enhance survivability is to complicate the attacker's targeting problems, i.e., develop a target system that will cause the enemy to expend his offensive capabilities without permitting functions essential to the defender to be neutralized. There are several ways of doing this, some of which include:

- Active efense;
- Hardening;
- Redundancy/ roliferation;
- Mobility;
- Cover and eception;
- Target voidance.

In order to measure the effectiveness of each approach, one needs to analyze the cost with respect to the number of warheads the enemy would have to expend in order to neutralize the target system. Though such a task is beyond the scope of this analysis a brief examination of each approach is included in order to provide a basis for thinking about their effectiveness.

Active defense. An old military cliché states that "the best defense is a good offense." If it is possible to attack an enemy before he attacks you and thereby severely degrade his ability to damage you, there will be strong incentive to launch a pre-emptive attack (as did the Israelis in 1967). In order to prevent such an option from being attractive, it is important to ensure that the enemy cannot gain anything from such

an attack and to avoid a situation where war appears inevitable.

Both the United States and the Soviet Union have expended a great deal of effort to prevent an attacker from being able to benefit from a pre-emptive attack. Efforts at reducing ICBM vulnerability are aimed at reducing this potential, as was the development of the strategic "triad." Consideration must also be given to protecting C^3I systems if pre-emption is to remain unattractive.

Another approach to an active defense that has been foresworn by both superpowers (to date) is the development of a means of destroying incoming enemy missiles. The Soviets have a very extensive anti-bomber system, but the Anti-Ballistic Missile (ABM) Treaty essentially prohibits the deployment of ballistic missile defense systems (BMD).[57] (It does allow a very limited one to be deployed.) In spite of the treaty, however, this option is getting much attention as other methods of insuring survivability of our forces become less effective and more costly.

Hardening. Before the advent of nuclear weapons, hardening was a common approach to the problem of survivability. As weapons became more powerful, concrete got thicker and holes were dug more deeply. The development of nuclear weapons, with their much greater destructive power, compounded the problem of protecting vital facilities. The lack of accuracy of delivery systems in the 1950's and 1960's made hardening continue to be worthwhile since it could provide protection against near misses. In order to ensure destruction of a target, a large number of weapons would have to be fired at the site. Before MIRV's were developed, attackers did not have enough weapons to assign large numbers to more than a few targets.

The deployment of MIRV's allowed several warheads to be placed on each missile, resulting in a tremendous increase in warheads. This increase, along with advances in warhead accuracy and yield, have made extensive hardening of limited utility. It is extremely difficult to harden a facility sufficiently to withstand a direct nuclear attack. For example, a 10 megaton warhead detonated on the surface will dig a crater over 400 feet deep and 3000 feet in diameter in solid rock.[58] Given the current and projected accuracies for weapons of this type it would not require a large number of warheads to literally "dig up" an underground target with nuclear explosions.[59] Even with improved accuracies, however, it could require several warheads to gain high probabilities of destruction for a deeply buried, "superhard" command posts. As a result, while attacking a few such targets (e.g., the ANMCC or the NORAD Command post at Cheyenne Mountain) would be feasible, as the number of such targets grew the required expenditure of warheads would rise rapidly.

Building "superhard" or even "hardened" facilities that would require the commitment of a large number of additional warheads to ensure destruction is very expensive, more so than the cost to the attacker of increasing the number of warheads, making this a futile effort. If arms control agreements limit the number of weapons, then this aspect of the problem would be less severe and such a program would have greater benefits.

Hardening can provide protection against threats other than physical destruction, however. "Electronic hardening" can protect C^3I facilities against enemy electronic counter-measures (ECM), such as jamming, as well as Electro-Magnetic Pulse (EMP). This type of protection is especially critical since both of these threats can affect a wide area. There-

fore, we cannot rely on the attacker "missing" nor benefit as greatly from deception or mobility.

Redundancy/proliferation. Increasing the number of targets requires the attacker to expend more and more weapons in order to get adequate coverage, thus redundancy provides another means of achieving "system" survivability. As I said earlier, it is not necessary for particular facilities to survive, but that the system be able to perform its required functions. This allows the defender to configure the systems so that it consists of many nodes and the loss of some of them does not destroy the integrity of the whole. For example, rather than one command post, numerous sites could be built each capable of performing the required function. In order to neutralize the function the enemy would have to destroy all the CP's. The same concept applies to warning systems or communications.

The cost of providing duplicate facilities is a critical concern, but can be influenced by what is contained in each location. Using our example of command posts, it is possible to "remote" many of the functions of the CP to widely separate locations, thus proliferating targets more cheaply. Rather than 10 command posts each with complete ADP facilities and communications equipment, presenting high value targets to the enemy, it is possible with modern communications to separate computer main frame from software and to use remote data bases. Communications equipment could be located elsewhere, with branches to the CP. By interconnecting all the facilities thus created, the number of targets in the system is increased and the value (and cost) of each is reduced. The cost of interconnecting the more austere facilities would have to be considered however.

Redundancy is more difficult to attain when considering the problem

of NCA survivability. In order to prevent the President from becoming an irreplacable "node" in the command structure, due to the restriction of release authority to him alone, the succession is defined for the NCA. Due to the sensitive nature of the President's responsibilities as release authority, successors below the vice president have seldom been thoroughly briefed on these responsibilities, and they are not accompanied by the release codes, as are the President and vice president.[60] As a result, their ability to quickly assume these responsibilities is limited. Another concern is that in day-to-day operations most of the successor are located in Washington, D.C. and could all be killed in a single attack on that city.

Mobility. Another old cliché states that "it is harder to hit a moving target." This applies to missile attacks as well as deer hunters. Given the lag time of intelligence, if a facility is mobile, the enemy will not be able to target it accurately. This concept is the basis for the decision to use airborne command posts. As long as they are airborne it is much more difficult to find and target them. Even with the advent of real time intelligence, the time of flight of missiles limits an attacker's ability to destroy a mobile target, even if it can be identified immediately.

By enabling a target to move out from under an attack, it does not need to be hardened against direct attack nor does there need to be a large number of nodes in the system to avoid destruction of its functional capabilities. Protection must be provided, however, against wide ranging effects such as EMP or loss of mobility, and sufficient numbers need to be available so that an attacker cannot disable the target by some special

operation. (For example, having a saboteur fire a rocket into the NEACP airplane as it sits on the runway at Andrews Air Force Base.)

Hiding/deception. If the attacker cannot find the target, he cannot destroy it. By disguising critical facilities, the enemy's targetting job becomes very difficult. The airborne command posts gain increased protection from the fact that it is difficult for enemy satellites to distinguish them from the multitude of planes in the air (in addition to the protection derived from being mobile). Many of the relocation centers for use by the government in time of nuclear attack are secret and hidden in buildings or underground tunnels. The effectiveness of this approach is limited, of course, by the ability to prevent the enemy from discovering their location. Improvements in satellite intelligence systems make it increasingly difficult to hide facilities. The openness of our society makes it even more difficult to conceal important fixed targets for long periods of time.

In addition to merely hiding a target, efforts at deception can be very useful. Military history is full of examples of successful deception programs. The concept of "multiple protective shelters" for the proposed MX missile relies on deceiving the Soviets as to which shelters, of many, contain missiles.

Target avoidance. Another early effort to enhance the survivability of C^3 systems involved the location of communications facilities away from cities and other presumed targets. This approach is similar to the idea of prolification in that the number of targets was increased. AT&T, which carries a great deal of military communications traffic, practiced a policy of target avoidance in its siting of switching facilities, and government

re-location sites were placed outside projected target areas.[61] This policy presumed that cities would be the likely targets in a nuclear attack. With the advent of MIRV's and the development of "counterforce" targeting concepts, this presumption may be no longer valid. In fact, a strong argument can be made that rather than targeting cities, city-avoidance will be the norm in a nuclear conflict. In a recent DOD study on war termination, it was determined that one of the important requirements to be met, if a nuclear war is to be terminated short of mutual destruction, is the avoidance of cities in an attack.[62] If a defender's cities are attacked, then he has little to gain from limiting the scope of retaliation.

One rather bizarre result of this situation is the potential for increasing C^3 survivability by locating facilities in major cities, especially those facilities required to conduct an extended conflict. The concept of disarming the defender while holding his cities as "hostages" to prevent massive retaliation becomes irrelevant if an attempt to disarm the defender results in the destruction of those cities. In such a situation the defender has nothing to lose by counter-attacking against the attacker's cities and therefore cannot be "blackmailed."

Combined approaches. Obviously, defense planners are not limited to using one approach. Often the most effective protection is gained by combining the approaches in order to further increase the attacker's targeting problem, since each concept suffers to some degree from the problem of diminishing returns.

An example of a mixed solution can be seen in the "race-track" approach to MX missile basing. It is impossible to make a silo hard enough to withstand a determined nuclear attack. Though it does greatly increase

the demands on the attacker to harden a silo to a certain degree, the attacker providing total protection would be very difficult and expensive. By proliferating the number of shelters, the enemy must expend more warheads than required to destroy one "superhard" silo. SALT could limit the number of missiles that can be deployed, so deception is used to hide one missile among 23 shelters. Since there is no guarantee that the Soviets will not penetrate the deception, the missiles are mobile so that they can change location before they can be attacked.

One final consideration should be kept in mind when thinking about survivability. At the risk of overusing trite phrases, "A chain is only as strong as its weakest link." The point is that C^3 effectiveness requires a total systems approach. Having survivable warning systems is useless if there remains no one to warn. Providing for NCA survivability is of limited utility if he cannot communicate with the surviving SSBN's.

Other survivability considerations. Another major consideration essential to the design of survivable C^3I systems is that of "graceful degradation." This refers to the way in which a system's capabilities gradually degrade rather than having damage to one segment result in total and immediate collapse. An analogy can be found in an examination of lighting systems. If lights are hooked up in series, when one light burns out the whole string goes out; by hooking them up in parallel, the loss of one light does not prevent the rest of the system from functioning. This problem is of particular concern to satellite designers. Since satellites are expensive to build and put into orbit and we cannot repair them (at this time at least), designers attempt to ensure that the loss of one function (e.g., a transponder on a communications satellite) does not

make the entire satellite useless.

Another factor that should considered when designing C^3I systems is the effect the system will have on the survivability of force elements it is designed to support. An example of this concern is found by examining communications to missile submarines. Current communications systems restrict the operating capability of these submarines because they are required to trail an antenna on the surface of the water. This restricts their speed and their operating depths. The Navy is concerned that improvements in ASW could enable the Soviets to detect these antenna and successfully attack our SSBN's. It is important to remember, therefore, that C^3I capabilities affect force capabilities and thus force objectives should be clearly defined before C^3I requirements are determined.

Credibility

Credibility is defined by Webster's dictionary as "capable of being believed; worthy of trust." The ability to provide information that is credible is critical to all aspects of C^3I. The two areas where it is especially critical are those of providing warning of an attack and transmitting release orders to the nuclear forces from the National Command Authority. One of the key questions that should be addressed in the case of warning is: "Can warning even be credible enough to support retaliation prior to enemy warheads actually detonating?" Given the incredibly high stakes involved, it can be argued that unless the warning system would be made completely error free, then warning information would not be credible enough to initiate a nuclear war. This concern has led to an emphasis on being able to allow the enemy warheads to explode before

initiating any irrevocable responses.[63] In 1976, however, Secretary of State Henry Kissinger raised the possibility of a "launch on warning" strategy, due to the potential vulnerability of our land-based missile force.[64] Should "launch on warning" ever be adopted, then credibility of warning will be especially critical.[65]

The credibility of release orders is also an important consideration. If we are to avoid accidental or unauthorized use of nuclear weapons, the recipients of release orders must be sure that these orders are authentic and come from the National Command Authority. This is a very sensitive aspect of nuclear operations and information regarding the means by which authenticity of release orders is assured is very closely held. Here again, credibility is aided by the policy of allowing an enemy attack to arrive before responding. Given this policy, the people who actually "turn the keys" to launch the weapons will be pre-disposed to question a release order in the absence of nuclear detonations and will have the opposite pre-disposition if they have experienced an attack.

Flexibility

Flexibility can be defined as "the ability to adjust to change; capable of being modified in order to readily adapt to changes in mission, organization, threat and technology."[66] In view of the rapid pace of technology, C^3I systems need to be able to adjust to new developments. Often cost is a key factor affecting flexibility. If a system is extremely expensive and has a long development time, it will be very difficult to abandon it in order to more effectively react to changes in threat.

The length of time needed to develop new capabilities and the

resulting requirement to "fix" technology at some point in order to complete the development is in constant tension with the desire to take advantage of the latest in technology. Trade-offs must be made between using low risk off-the-shelf technology that may become outdated quickly, or developing high-risk technology that, while promising greater capabilities, results in additional delays and possible problems.

One of the reasons that designers desire to be on the forefront of technology is due to the uncertainty they face with respect to increases in threat capabilities. Since there are many needs, all competing for limited budgetary resources, deciding how much to spend on anticipating events can be difficult. Using the example of the submarines again, the probability of the Soviets improving their ASW capability enough to detect the antennas trailed by our SSBN's is not very high; but if they should be successful, the consequences could be serious. The question becomes: "How much should we hedge our bets by buying a partial improvement now, rather than taking a long time to obtain a more complete solution to what is now only a potential problem?"

The military forces of this nation must be capable of a wide variety of operations in situations which vary from peacetime to local crisis to world war. Since it would be incredibly expensive and wasteful to have different C^3I systems for each level of operations, systems must be flexible enough to support a variety of missions. For example, intelligence satellites not only detect ICBM launches, they also measure wheat crops and monitor activities of conventional forces. Often the requirements of one mission affect the ability to perform another, so judgments must be made regarding whether a particular capability can be degraded in order to

perform a wider variety of tasks or more money spent for additional capability. Day-to-day needs often overshadow the more serious, but infrequent, requirements generated by crises or wars. Since effectiveness in routine operations often determines promotion, managers can tend to focus on those needs to the detriment of more serious ones.

Responsiveness

The definition of responsiveness, "the ability to react within necessary time and quality criteria," emphasizes the importance of determining the time and quality parameters if the concept is to be meaningful.[67] The tendency when developing C^3I systems is to attempt to maximize responsiveness, sometimes without a clear examination of what the criteria are or why they are chosen.

Time and quality criteria are often in conflict. If the quality of the output is to be high, there is a need for methods of checking these outputs--which takes time. For example, if warning information is to be meaningful to the NCA, it must be assessed and evaluated. If its accuracy is to be insured, it must be checked and corraborated. These requirements conflict with the desire to minimize the delay in notifying the President of an attack.

Responsiveness also influences survivability requirements. A highly responsive C^3I capability enables the nuclear forces to perform their functions before an enemy can destroy them, thus reducing the need for them to be able to endure an attack.

The survivability of the forces being supported also influences the need for responsiveness. The vulnerability of bombers and the increasing

vulnerability of ICBM's impose a greater need for responsiveness on C^3I systems than does the more secure SSBN force. Unless an attack can be detected and orders sent to launch the bomber forces within a few minutes, this leg of the triad would be destroyed on the ground. The ability to recall bombers once they are launched enables responsiveness to take precedence over credibility; in the case of ICBM's, this is not so.

The degree of responsiveness needed is also a function of the mission of the force in question. If the targets of the retaliatory force are time critical, then a very responsive C^3I system is required; if not, considerations such as survivability and credibility may take precedence. The important point is that--without asking questions about force missions and capabilities--one cannot accurately determine C^3I requirements.

Security

Security, with regard to C^3I, can be defined as "the ability to act with confidence that current and projected plans will not be compromised."[68] In an open society, secrecy is always difficult. Among our most closely guarded secrets, however, relate to the procedures for command and control of our nuclear forces, as well as the methods of collecting intelligence concerning enemy activities in this area. Enemy knowledge of intelligence methods would better enable them to devise ways to deceive our warning systems and enhance the effectiveness of a surprise attack. It is possible to overdo the concept of security, however, to the point where our own ability to act is hampered due to the inadequate or improper dissemination of information. Reconciling these two concerns is one of the most fundamental security problems.

Integration

A "systems approach" is essential when designing C^3I capabilities. Though we have referred to various C^3I "systems," they are all actually elements of a larger system that meets all the requirements outlined in the section, C^3I FUNCTIONAL REQUIREMENTS. It does little good to enhance the capabilities of one element if such an improvement is not integrated with the capabilities of other elements. For example, the development of a new warning system--which can provide tremendous amounts of data about enemy activities very quickly--is useless if the communications system is incapable of transmitting the information to a decision maker or if the information handling capabilities preclude effective processing.

The capabilities and limitations of each element in the overall C^3I system must be integrated if we are to avoid wasteful unused capacity in some elements--and bottlenecks in others.

Reliability

A recent GAO report on the Worldwide Military Command and Control System (WWMCCS) defined reliability as "the characterization of an item expressed by the probability that it will perform a required function under stated conditions for a stated period of time."[69] What this definition says, in essence, is that reliability means the ability of a system to work when needed. A sophisticated, advanced, highly capable system is of little use if it cannot be depended on to operate effectively when required.

Efforts to increase reliability are often in conflict with the desire to use the latest technology and the need to reduce costs. The development and deployment of the latest "state-of-the-art" system often

requires a period of "debugging" before it becomes reliable. Trade-offs must often be made, therefore, between a desire for reliability and new, unproven methods that promise greater capabilities.

Reliability often requires such things as back up systems and high quality equipment. Efforts to keep costs low tend to result in the elimination of redundancy and reduction in quality. While initial savings may be achieved, effectiveness can be degraded. Too often the orientation during development is on getting the greatest capabilities per dollar; as a result, after deployment, the focus is on getting the most reliability per dollar. Some planners feel that once a system is operational, the money will be there to make it reliable; whereas if reliability is a design goal, the costs will rise and the program be cancelled. This approach can cause serious problems--and does.

CURRENT C^3I SYSTEMS

Now that we have examined the factors that influence C^3I requirements, determined what the major requirements are, and considered what qualities are needed to meet these requirements, we now turn to a brief overview of current C^3I systems in order to gain an understanding of what capabilities and problems exist.

The move toward centralization of command and control of the strategic forces (in fact, all military forces) stimulated by JFK's insistence on firm and complete civilian control, and the growing Soviet threat, led to the development of an integrated C^3I system which was designed to meet the requirements discussed earlier. Out of this development effort came what is known today as the Worldwide Military Command and Control System (WWMCCS). In a recent report, the Government Accounting Office described this system (called "WIMEX") as "an arrangement of personnel, equipment (including automated data processing [ADP] equipment and software), communications facilities, and procedures, employed in planning, directing, coordinating and controlling the operational activities of U.S. military forces."[70] WWMCCS provides the President with the information he needs for decisions and the ability to transmit those decisions directly to the executing forces. It is the major element of strategic command and control, and one of its primary tasks is to provide for the direction of the nuclear forces in the execution of the SIOP. We shall examine the three major categories of systems within WWMCCS:

- Warning and Surveillance Systems;
- The National Military Command System (NMCS);
- Communications Systems.

Warning and Surveillance Systems

There are several warning systems that have been developed to meet the varied threats posed by Soviet ICBM's, SLBM's, and bombers. In the 1950's, the U.S. only had to worry about bombers. To counter that threat we built the DEW line consisting of 31 radars in Alaska and Canada in the mid-fifties. These radars provided approximately two hours warning of an impending Soviet bomber attack.[71] They are still in use today but are supplemented by other systems, including an airborne radar system called "AWACS." Though AWACS was not originally designed for strategic early warning, its ability to detect low-flying bombers, which the DEW line cannot, makes it a valuable element in the warning system.[72] In another effort to improve bomber warning, the Defense Department is continuing development of an over-the-horizon "backscatter" radar (OTH-B) that will provide greater range than current systems. It cannot replace the DEW line, however, as it is adversely affected by auroral effects. (It will be used on the coasts.) Improvements to the DEW line are also being examined. Space-based bomber detection systems are being experimented with, though so far results are limited.[73]

In 1957, in response to the developing ICBM threat, the U.S. constructed the Ballistic Missile Early Warning System (BMEWS) which consists of three sites (Alaska, Greenland, and the U.K.) designed to detect the approach of Russian land-based missiles. This system, now over 20 years old, remains an integral part of our warning network, though it is getting to be difficult to maintain and expensive to operate (its IBM 7080 computers are obsolete and no longer produced). The Perimeter Acquisition Radar (now called "PARCS") that was formerly part of the single SAFEGUARD installation has also been integrated into the ICBM warning system.

To counter the threat posed by Soviet SLBM's, the U.S. developed and built six SLBM warning radars (474N) in the 1960's which have become obsolete and are being replaced by two "PAVEPAW" phased array radars (one on Cape Cod and one in California).[74] In addition, the primary mission of the phased array radar at Eglin Air Force Base in Florida is being changed from tracking space objects to SLBM detection.[75]

A third surveillance function provided by ground-based radars involves the detection and tracking of space objects to determine potential hostile intent for targeting by future ASAT systems. There are over 4,500 space objects that are tracked by surveillance radars located in the U.S. and in Turkey.[76]

The object of our tactical warning systems is to provide not only redundancy, but also "dual phenomenology" coverage of all potential ICBM and SLBM approaches. To do this we have augmented the radar system with satellite sensors. These satellite early warning systems provide the earliest warning of an enemy attack, while the radar systems provide confirmation and assessment. The Defense Support Program (DSP) consists of three early warning satellites which utilize thermal sensors to detect infrared emissions from the exhausts of ICBM's or SLBM's.[66] Though the DSP satellites can detect an attack more quickly than the ground-based radars they can be "spoofed" by sunspots, large fires, or possibly enemy activity, thus the reliance on dual phenomenology to prevent errors.[78] Even so, there are some false alarms--a problem that will be discussed later.

Much has been heard about our "spy" satellites that take detailed aerial pictures of the Soviet Union. Though useful for providing strategic warning indications, the lag time involved in processing the information

from these systems makes them of limited use for providing warning of an immediate attack.

The SLBM threat is of particular concern to U.S. defense planners due to the short flight time of these missiles. In an effort to remedy this problem, Secretary Brown is looking at a new satellite system called the "Mosaic Sensor Program" (MSP) which will detect SLBM launches faster and more accurately than the current DSP system. The MSP satellites would also provide an ability to accurately determine launch points of Soviet ICBM's and SLBM's, thus identifying empty silos and providing re-targeting information to U.S. planners for a retaliatory strike.[79] The spy satellites mentioned above provide some capability to determine this information but would take longer to do so. The new satellites would also provide for on-board processing of information, which would allow smaller ground terminals. These terminals could be made mobile, hence more survivable.[80]

Survivability is a major problem with the current warning systems. The radar sites are not hardened and are limited in number (there are 53 sites, but 31 can only detect bombers); they could be neutralized by nuclear or conventional attack, or by sabotage or paramilitary activity very quickly. The DSP satellites are more survivable (ASAT interceptors would take hours to reach them but they could possibly be "blinded"), but currently all DSP satellite information is received by only two large earth stations, both of which are vulnerable to the threats mentioned above.[81] It would be 1984 before the MSP satellites could be deployed to solve this problem, if Congress approves current budget requests.

Another system that is in development to improve attack assessment

is the Integrated Operation Nuclear Detection System (IONDS). This system is designed to detect nuclear explosions and pinpoint their locations. It will aid in attack assessment during a Soviet strike, enabling the President to characterize the attack accurately and determine an appropriate response. It will also provide damage assessment after a U.S. retaliatory strike to help U.S. planners with targeting. The IONDS system has been approved and will go on the 24 Global Positioning Satellites that will soon be launched.[82]

One of the concerns that continues to be a problem with our warning system is false alarms. These can be a result of sensors receiving wrong information and passing it along, or they can be generated within the computer system by errors. In either case they affect the credibility of the warning system. Though the problem of a false alarm causing a U.S. retaliation is reduced by our ability to wait until detonations occur before responding, a reduction in the credibility of the system can slow reaction to a threat due to doubt over its validity. Recently a false alert was caused by erroneous data being fed into the computer network accidently. A low-level alert was initiated and lasted six minutes. Pentagon officials said that several false alarms had occurred in the past few years due to computer failures, Soviet test firing, and natural phenomena such as sunspots.[83]

In the most recent incident, an alert went out from NORAD to command centers throughout the nation, but B-52 bombers were not ordered into the air, nor was the President notified (though if it had lasted another minute he would have been) in the six minutes before a mistake was noticed.[84] This may be an indicator that errors have already affected the responsive-

ness of the system. Given the short flight time of SLBM's to Washington or the bomber bases, delays in response to a warning--because "wolf has been cried too often"--could have serious consequences. There was considerable concern shown by the media, especially in the United Kingdom, about the possibility of an accidental war being caused by such an incident.[85] Though that is an important problem, current doctrine provides safeguards against such an occurrence. These two views point up the inherent tension that exists between the need for responsiveness and concerns about credibility and reliability.

National Military Command System (NMCS)

The NMCS is the priority sub-system of the WWMCCS. It is designed specifically to support the NCA, and in addition supports the JCS. As we noted earlier the chain of command does not coincide with the statutory chain of command; the JCS is part of the communications chain, though they have no statutory authority.

The chairman of the JCS operates the NMCS for the Secretary of Defense. He has been delegated responsibility by the secretary for the following:

- Defining the scope and extent of the NMCS;
- Developing and validating requirements for the NMCS;
- Establishing NMCS operational policies and procedures.[86]

The chairman of the Joint Chiefs of Staff provides the military staff to the NCA, advises the NCA, provides the channel of communications from the NCA to the executing commands, and coordinates the communications to the unified and specified commands. Being a part of the communications chain

endows the chairman with more influence than he would otherwise have.

The NMCS consists mainly of the national command centers and the communications linking these centers with the executing commands and the surveillance systems. At the command centers information is processed and put into a form to facilitate decision making by the NCA. The input for these decisions comes from the surveillance systems discussed earlier, and the reports of friendly force commanders. The processing of this information requires extensive automatic data processing (ADP) capability. To handle this task WWMCCS utilizes 35 Honeywell 6000 series computers located at 27 sites.[87] While this network handles the bulk of data processing, the NMCS is not totally dependent on it for information. Critical information on an enemy attack can be transmitted outside the computer system, though data processing capability is limited.[88]

Information processing is currently one of the major problem areas in WWMCCS. The system, designed in the 1960's, uses computers that have become obsolete in the rapidly advancing computer industry and suffers from a variety of problems. A recent GAO report listed several deficiencies in the WWMCCS ADP system, a program on which the government has spent over one billion dollars. These problems include:

- The ADP System is not reliable and is especially prone to breakdowns during crisis;
- Lacks effective and economic growth potential;
- Lack of back-up systems;
- ADP equipment is not installed in survivable facilities, and supporting utilities in many cases are vulnerable to sabotage.[89]

One of the major reasons for the problems, according to the reports, is that the management structure is so fragmented, no one has a complete overview of the program or the responsibility for its management.[90] Before

improvements can be made, organizational problems must be dealt with.

The results of recent command post exercises seem to corroborate the GAO charge that WWMCCS is unreliable, as problems occurred which limited the effectiveness of the system.[91] Though WWMCCS managers claim that overall reliability has improved to about 94 percent, they admit that the lack of a back-up system is a problem and that the system is prone to problems during a crisis, precisely when it is needed most.[92]

Given the volume of information needed to meet the C^3 requirements we articulated earlier, the lack of reliable information systems based on ADP equipment could affect the ability of the NCA to make rapid decisions, and as a result, limit the options available to the President in the short run. This puts a higher premium on the endurance of C^3 systems in order to survive long enough to support slower decision making.

Another problem mentioned in the GAO report is the lack of systematically identified information requirements. In order for the system to provide useful data, the information needs of the NCA must be clearly specified. In order to do so, top level user participation is required in the validation of the outputs of the system. Otherwise, there is a tendency for system designers to develop outputs that conform to the capabilities of an automated system rather than user needs. The result would be that the decision maker could be inundated with useless information.

The warning and information networks feed into three main command centers that are part of the NMCS. These are the National Military Command Center (NMCC) at the Pentagon, the Alternate National Military Command Center (ANMCC) at Ft. Ritchie, Maryland, and the National Emergency Airborne Command Post (NEACP) which provides an aircraft at Andrews Air Force

Base in Washington for the President. Day-to-day and crisis management operations are conducted from the NMCC in the Pentagon. This is an unhardened facility that monitors the operations of U.S. military forces around the world as well as the warning and intelligence systems. Since the NMCC is not expected to survive an enemy attack, the ANMCC provides a remote, hardened facility that can be rapidly augmented with personnel to assume control of operations. Critical data at the NMCC is also located at the ANMCC to provide instantaneous assumption of control if needed. It is tied to the NMCS data base and has communications to all the other command centers. Though hardened, it could not be expected to withstand a direct attack either. Therefore, NEACP--a third command center--has been established.

The National Emergency Airborne Command Post (NEACP) is designed to provide a survivable command center for the NCA during a nuclear attack. The NEACP is located in a 747-type aircraft and is deployed at Andrews Air Force Base. If an attack were imminent, the President could board NEACP and operate from it while airborne. The E-4A's, as they are called, replaced earlier 707-type aircraft that are still used to provide Airborne Command Posts for the unified commands. These aircraft provide extensive communications capabilities to enable the President to maintain contact with his forces. The radio equipment is designed to operate in ECM environment as well as provide secure voice capability. The E-4's are also linked to communications satellites through an on-board terminal. In addition to communications facilities, the NEACP also provides space for a staff to accompany the NCA in order to process information and assist in planning. One limitation of the current aircraft is their lack of ADP

equipment on board. Dr. Dineen pointed out this lack when he stated that it was filled with "a bunch of filing cabinets" and that, "to generate various options the President's staff would have to go to the file cabinets and do things basically by hand."[93] Lack of ADP equipment will hamper the responsiveness and flexibility of our response to attack, given the large amounts of information involved in attack and damage assessments. To rectify this problem Secretary Brown has directed the Air Force to install ADP capability in the first E-4 by December 1981 at an estimated cost of $31.4 million dollars.[94]

Another problem confronting the NEACP is vulnerability to EMP. Given the widespread EMP effects from an exo-atmospheric burst--even if the aircraft escapes from Washington, it could be neutralized by EMP from a nuclear blast hundreds of kilometers away. To correct this vulnerability the four E-4 aircraft are being modified with EMP protection. One E-4B aircraft has been completed and the administration has included funds for modification of one aircraft in the fiscal year 1981 budget. The conversion of the other three is also planned, as well as the purchase of two additional aircraft by fiscal year 1983.[95]

Among the problems with NEACP that have not been solved are:

- The limited endurance of the aircraft. After approximately 20 hours it will have to land or face the potential of engine failures.[96]

- There are a limited number of runways that can accommodate 747's in the U.S. and the enemy could target these to prevent landing. It should be noted that these runways are in major airports near large cities so targeting them would cause extensive collateral damage and tend to change the character of an enemy attack from counterforce to counter-city, thus increasing the probability of escalation.

- The NEACP cannot operate its communications facilities effectively while on the ground.

· The NEACP aircraft is susceptible to sabotage.

In view of these continuing problems the NEACP can be expected to provide an added degree of survivability to the NCA, but only for a limited time period.

The above comments assume that the President reaches his Airborne Command Post. Andrews Air Force Base is an eight-minute flight from the White House by helicopter (assuming the helicopter was already at the White House, which they are not normally, though presumably in a crisis they would be). Estimates of time of flight for an SLBM fired from off the East Coast range from 6-12 minutes.[97] Even using the 12-minute figure, we would have to identify, process, and transmit an attack warning to the President within four minutes for him even to reach the plane, let alone fly to safety.

In addition to the national level command posts of MNCS, there are four additional airborne command posts for CINCEUR, CINCLANT, CINCPAC, and CINSAC, that are capable of communicating with the nuclear forces. While the others use EC-135 (707-type) aircraft, the SAC Airborne Command is an E4-A aircraft stationed at Offult Air Force Base, Nebraska. It is the only airborne command post (ABNCP) that is constantly airborne, and it has a general officer and battle staff on board to insure survivable command and control.

The SAC ABNCP is responsible for control of the ICBM's and B-52's while the LANTCOM and PACOM ABCNP's are responsible for SSBN's (CINCEUR has only theater nuclear forces). But Emergency Action Messages (EAM), the orders to launch an attack, can be originated at any one of these CP's as well as from NEACP, the NMCC, and the ANMCC.[98] The President does not

have to go through the nuclear commanders to have EAM's executed. He is capable of communicating directly with Launch Control Centers (LCC'S) in the missile fields, the B-52 crew or SSBN's. Any of the ABNCP's have the capability to do so though they are restricted by the range of their communications equipment.

Merely communicating with the nuclear forces is not sufficient to launch nuclear weapons, however. The prevention of accidental or unauthorized launching of nuclear weapons has been a major concern since they were introduced, and it has an important impact on command and control procedures making the process of nuclear release more complex. The procedures designed to prevent unauthorized launch of nuclear weapons are designed to address two aspects of this problem: preventing executing personnel from launching missiles without authority and insuring that orders to release weapons originate from the National Command Authority.

To prevent the officers manning an ICBM launch control center (LCC) from launching the missiles under their control, the concept of multiple-person-control is employed. Both officers in the LCC must verify launch orders and turn separate keys to activate the launch mechanism. The location of the keys prevents one person from turning both simultaneously, as is required. Another two-man team, in another LCC, must take the same actions, and to complete the launch sequence, a "launch-enabling code" must be received from SAC Headquarters. Should this facility be destroyed, the capability would automatically switch to one of 80 other SAC command posts, both ground-based and airborne.[99]

On missile submarines, the launch of SLBM's also requires the concurrence of several people. To launch a missile, four officers in dif-

ferent parts of the ship must turn keys or throw switches. There are no controls outside the submarine, however.[100] Since planes may be "launched on warning," procedures have been established to maintain "positive control" while in the air. After taking off, the planes fly to a specified location where they circle and wait for orders authorizing them to proceed to their targets. This message must be authenticated by three officers (two on FB-111's) or the plane returns to base. As with missile submarines, there are no external controls on the crew.[101]

The other side of the problem is insuring that the person originating launch orders is authorized to do so. To prevent this from happening special codes are required to initiate an authentic EAM, which will release the nuclear forces. The President and vice president are accompanied everywhere by a military aide that carries these sealed codes. While the President's ability to release nuclear weapons is not totally dependent on use of the authentication codes, the lack of such codes would seriously hamper operations. Without launch enabling codes the ICBM's could not be fired, but SLBM's and bombers would be unaffected.[102] The exact locations of codes and the precise limitations on launch capabilities are highly classified, but a consideration in C^3 planning must be to insure that the enemy cannot identify and eliminate a small number of code locations thereby paralyzing our ability to launch weapons. This concern demonstrates one of the fundamental tensions between the desire to centralize authority to prevent accidents and a desire to prevent the creation of small numbers of especially lucrative targets that could be destroyed--thus neutralizing the entire system.

Communications Systems

In order to ensure that the nuclear forces will receive the Emergency Action Message (EAM) in event of a nuclear attack, an extensive communications system has been developed as part of WWMCCS. In order to increase the probability of an EAM being communicated, redundant systems are used.

Communications to ICBM's. Communications to the ICBM force have a greater degree of redundancy and variety than those systems supporting bombers, and SLBM's. As a result command and control is tightest over this leg of the triad. This is due, in part, to the greater ease in communications afforded by the fact that ICBM silos are fixed ground sites. The various methods include:

- Radio messages from ABNCP's;
- Radio messages from ground facilities;
- Emergency Rocket Communications Systems;
- Radio messages via satellite;
- Commercial and military telephone networks.

1. Airborne radio systems. The ABNCP's have an impressive array of radio equipment for communications with the nuclear forces. The facilities include: high-power, very low frequency (VLF), and low frequency (LF) radios, primarily for communications with SSBN's and TACAMO, as well as high frequency (HF), ultra high frequency (UHF) radios, and super high frequency (SHF) satellite terminals for communications with ICBM's bombers, and other ABNCP's. These systems provide secure voice and anti-jam capabilities.

The HF and UHF radios give an only line of sight capability, but due to their location in airborne platforms their range is extended, enabling them to communicate with other aircraft such as bombers or ABNCP

The SHF satellite terminals are designed to provide long range communications to LCC's and other ABNCP's, though these facilities have HF UHF capability also. The range limitations of UHF and HF necessitate the use of relay aircraft in order for NEACP to talk to the SAC ABN CP or the LCC's. The VLF and LF systems provide a low-speed link beyond line of sight between ABNCP's as well as to TACAMO and SSBN's. These will be discussed in more detail with TACAMO.

One of the limitations of these airborne systems is the small number (14) of ground entry points (GEP) that allow ground-based wire communications to interface with the airborne radio nets. If the NCA is not aboard an ABNCP he could have trouble communicating with them if these GEP's are knocked out.[103]

The Post-Attack Command and Control System (PACCS) includes the relay aircraft, mentioned above, the SAC uses to link the NEACP and SAC ABNCP to the widely dispersed bombers and ICBM bases. These are EC-135 aircraft with HF, UHF, and LF capabilities.

These airborne radio systems are part of the Minimum Essential Emergency Communications Network (MEECN). MEECN is a collection of systems designed to provide a backbone of survivable communications to all three legs of the triad.

2. Ground radio links. In addition to these aircraft, SAC has a variety of ground-based radio systems used to transmit alert messages and EAM:

- The Primary Alert System (PAS);
- SAC Automated Command and Control System (SACCS);
- GIANT TALK Single Side Band/HF radio network;
- GREEN PINES, a UHF radio network.

3. Emergency Rocket Communication System (ERCS). The Emergency Rocket Communication System uses a Minuteman ICBM with radio transmitters, instead of a nuclear warhead, in their nose cones. Should other communications systems fail, the EAM can be sent by firing the ICBM in a trajectory that would enable other IXBM fields to receive its transmissions. The advantage of this system is that the transmitters are located in hardened missile silos to increase their ability to survive a nuclear attack. ERCS does have several limitations, however. ERCS wing is located at Whiteman Air Force Base in Missouri. Dr. Dineen, in testimony before Congress in 1979, admitted that we would have to assume that the Soviets could know where the ERCS missiles were located and could target additional missiles to insure they are destroyed.[104] It is possible to change their location, however. If a shell game were played with ERCS, it would be more difficult for the Soviets to identify them accurately and single them out for special targeting attention, since ERCS silos look no different than regular ICBM silos. Testimony by defense officials indicate that this is done to a limited extent.[105]

4. Satellite communications. Satellites are becoming more and more important in military communications. Several satellite systems currently provide communications in peacetime to the nation's military forces. The major system -- GAPFILLER, FLTSATCOM, and Defense Satellite Communications

System (DSCS) -- are not designed to survive a nuclear attack, but they are multi-purpose systems and are important to strategic C^3 because they provide platforms for the AFSATCOM system.[106]

AFSATCOM is designed to provide communications to all the strategic nuclear forces. It uses the satellites currently in orbit with FLTSATCOM and GAPFILLER and will be put on the DSCS satellites in the early 1980's. On each satellite one or more "transponders" (the element that receives and transmits signals from/to earth) are dedicated to the AFSATCOM mission and link airborne terminals on ABNCP's, bombers, as well as ground terminals at LCC's, and command centers. These terminals are being installed in fiscal year 1980.

By putting AFSATCOM transponders on a large number of satellites, rather than having a few dedicated satellites, greater redundancy is achieved, thus complicating Soviet ASAT efforts. The emphasis on redundancy is due to the difficulty involved in adequately hardening satellites against an ASAT threat. In addition to the proliferation of targets, another means of increasing the endurance of the system is to "hide" satellites in orbit. These platforms would not be activated until after the operational platforms were destroyed; therefore it would be very difficult to detect among the large number of objects in orbit around the earth. These satellites would need to be hardened against EMP, however, due to the wide coverage of this threat. The major threats to satellite communications are as follows:

- Destruction of space platforms (ASAT);
- Destruction of ground terminals;
- Jamming;
- Nuclear effects (EMP, blackout).

The proliferation of satellites and use of hidden back-ups reduces the threat to space platforms and the deployment of airborne and mobile terminals makes it difficult to neutralize these portions of the system. Anti-jam capabilities are being added to satellite transponders to reduce the vulnerability to enemy ECM. EMP hardening is also being done, but atmospheric disturbances could still cause significant degradation in satellite communications.

5. Telephone networks. Reliance on radios could be a problem in an environment where the atmosphere has been ionized by numerous nuclear blasts. The communications links to the ICBM's and bombers are not limited to radio, however, as the ground command posts are linked by telephone to the land-based forces. The airborne command posts are also able to enter the ground-based networks via 14 ground entry points.

The United States has the most sophisticated and widespread telephone network in the world with potential to provide numerous diverse routes from NCA to the nuclear forces. AT&T and the Defense Department cooperated in the 1950's and 1960's to increase the survivability of the telephone system. Critical switches and facilities were sited to avoid targets, and in some cases hardened. Though the network density provides great potential for survivability through use of redundant facilities and routes, the configuration of the system and the industry prevents maximum use of this potential.

Recent advances in technology have led AT&T to consolidate switching facilities and other critical network facilities, making the system dependent on a relatively small number of nodes that are vulnerable to attack. While concepts such as packet switching provide the potential

for network de-centralization hence greater survivability, the trend is towards centralization, making the system more easily disrupted.

Though AT&T makes up the bulk of the telecommunications capacity of the country, other firms have facilities that contribute to the communications resources potentially available in an attack. These systems are not capable, at present, of being interconnected except at a few points. This greatly reduces their value, as in the aftermath of an attack we could expect unconnected pieces of each to survive, but reconstitution would be hampered unless the pieces could be connected to form a new network.

Ground-based telecommunications offers some advantages and disadvantages when considered for strategic communications in a conflict. Communications via cable or microwave offer some advantages with respect to security, resistance to jamming and atmospheric disturbances, as well as tremendous capacity. These advantages are offset by the vulnerability of their fixed nodes to attack and vulnerability to EMP. Improving commercial networks is an option that should not be ignored in discussions of C^3 upgrades. This is especially true if the broader needs of the nation in a nuclear conflict are considered.

Communications to bombers. The communication systems to bombers are the same as those to ICBM's, with the exception of the telephone networks. The primary methods of bomber control are via HF and UHF radio. The B-52 force is also being equipped with satellite terminals to augment the radio systems, thus enabling communications at much greater range. This is important if bombers are to be used in a damage assessment role.

Communications to SSBN's. Missile submarines are the most survivable portion of the nuclear triad and, therefore, comprise a major portion of the secure reserve force. The need for these submarines to remain hidden in order to avoid Soviet ASW action limits our ability to communicate with them since they must remain submerged. Radio waves in the higher frequencies cannot penetrate the ocean's surface. This creates a problem since, according to the Director of Navy C^3, Rear Admiral Nagler, "In order to be responsive to NCA orders, SSBN's in day-to-day alert readiness postures must maintain continuous communications reception."[107]

1. Current systems. The current systems used to communicate with submerged SSBN's include:

a) Ground-based systems. The Navy has two shore-based VLF transmitters on the East Coast and one on the West Coast. These serve as the primary means of communicating with SSBN's. There are also a limited number of low frequency (LF) and high frequency (HF) transmitters located on shore stations around the world.

b) Ship-based HF systems. All Navy ships utilize HF radios for tactical operations. These systems can also be used to relay messages from shore stations to nearby SSBN's.

c) UHF satellite systems. GAPFILLER and FLTSATCOM satellites provide a two-way, high-speed, communications link to SSBN's. The shore-based links of these systems are fixed satellite terminals.

d) TACAMO. This system uses 12 modified C-130 aircraft stationed on Guam and Bermuda. The TACAMO aircraft have HF, VHF and UHF facilities for communications to other aircraft, as well as a satellite terminal which links it to AFSATCOM and FLTSATCOM. TACAMO's primary link to SSBN's is via

a VLF transmitter on board. This system uses a long wire antenna (which is over 10,000 feet long) which the plane trails out behind it while flying in a tight circle (to keep the wire verticle).[108] It can also talk to SSBN's at shorter range via HF.

2. Problems with current systems. Current communications links to SSBN's suffer from several problems:

a) Range. The current systems suffer from range limitations, resulting in a need for additional facilities and relays. VLF has the longest range, but still requires that TACAMO aircraft be deployed in each ocean. Range of HF and LF systems are more limited, requiring the deployment of overseas transmitters. While numerous transmitters increase the enemy's targeting problem, their limited range does not allow much redundancy in a specific geographical area.

b) Survivability of communications facilities. Only TACAMO is considered to be a survivable system in event of war.[109] In order to be survivable one of the TACAMO aircraft stationed in the Atlantic area is constantly airborne; lack of sufficient aircraft prevents continuous airborne alert in the Pacific but one aircraft is on ground alert at all times, prepared to take off on a 15-minute notice.[110] The administration has requested four more aircraft, so that when TRIDENT is deployed to the Pacific a continuous airborne capability will be available there, as well as to replace some aging airframes. The fixed shore-based sites are not hardened and could be destroyed not only by nuclear attack, but by sabotage or conventional attack as well.

c) Need for surface antenna on SSBN's. VLF radio signals can only

penetrate seawater to a depth of a few meters, HF and UHF signals will only penetrate a few centimeters. In order to receive messages, a submerged SSBN must either trail an antenna near the surface for VLF, trail a buoy on the surface for HF, or extend an antenna above the surface for UHF. As a result of this requirement, the operational capability of SSBN's is restricted. Submarines must cruise near the surface and can only operate at reduced speeds in order to trail a floating wire antenna over 2,000 feet long within 20 to 30 feet of the surface.

Though the SSBN force is not currently threatened by Soviet Anti-Submarine Warfare (ASW) technology, the Navy is worried that ASW advances could jeapordize the security of the sea-based deterrent.[111]

d) Jamming. Soviet jamming poses a significant threat to our ability to communicate with SSBN's. Efforts are being made to increase the resistance of the current communications, but the problem continues to be of concern.

Communications with adversary leadership. Though not an explicit mission of our strategic C^3 systems, the ability to communicate with the enemy may be critical in order to terminate nuclear conflict. As Secretary Brown stated to Congress, "In crisis and war, maintaining continuous communications with adversary leaders would serve to clarify events and control escalation through negotiation."[112] While much effort has gone into insuring communication to fight the war, less effort has been made to insure a communications needed for termination are maintained. As a result of past crises, the U.S. and U.S.S.R. have established a teletype link between Washington and Moscow called MOLINK (more commonly referred to as the "hot line"). This system is not designed to survive a nuclear

attack, however. Given the potential for widespread destruction and rapid operations, exchanging notes through diplomatic channels does not seem a realistic approach. While this problem may not be our most important communications concern, it is significant.

NOTES

1. Department of Defense, Department of Defense Directive 5100.30 The World-Wide Military Command and Control System (WWMCCS), (Washington, D.C., 1974), p. 2.

2. C. M. Herzfeld, "Command, Control, and Communications," Adelphi Paper, 145:40 (Spring 1978).

3. Executive Order 12036 entitled "United States Intelligence Activities was issued by President Jimmy Carter on January 24, 1978.

4. From a speech by Secretary Dulles to the Council on Foreign Relations, New York City, January 12, 1954. See The Use of Force, Robert Art and Kenneth Waltz, editors (Boston, 1971), p. 128.

5. From a speech by Secretary McNamara delivered at the University of Michigan on June 16, 1962. See Art and Waltz, p. 134.

6. Thomas C. Schelling, Strategy of Conflict (London, 1960), p. 9.

7. Department of Defense, Department of Defense Annual Report FY 1981 (Washington, D.C., 1980), p. 65.

8. Ibid.

9. The objectives were taken from comments by General Rosenberg, a staff member on the National Security Council during a seminar at the John F. Kennedy School of Government.

10. The Stanford Research Institute study, A Retrospective Look at Some of the Basic Issues Connected with National Command, Control and Communications has a good discussion of doctrine and C^3I requirements.

11. From testimony by Dr. Gerald Dinneen, Assistant Secretary of Defense (C^3I). See Committee on Armed Services, Senate, Hearings on DOD Authorization for Appropriations for FY 1980, Part 6, 96th Cong. 2nd Sess., (Washington, D.C., 1979), p. 3353. Hereafter referred to as "FY 1980 R & D Hearings."

12. Roger Hilsman, The Politics of Policy-Making in Defense and Foreign Affairs (New York, 1974), p. 50.

13. Bruce G. Bowers, "Civilian Control of the Military: Historical Precedents for Today's Realities" (Air War College, 1978), pp. 3-7.

14. Ibid., pp. 10-20.

15. President Polk wanted to annex what is now part of the American Southwest and ordered military operations rather than concentrating

forces under General Scott at Veracruz. President McKinley's concern for the international political situation caused him to prevent the Navy from sending a fleet to attack the Spanish Coast.

16. Bowers, p. 26.

17. Robert D. Adams, et al., "Command and Control Systems Evaluation and Management" (Air War College, 1974), p. 36.

18. Ibid.

19. Robert F. Kennedy, The Thirteen Days (New York, 1969), pp. 48, 119.

20. Section 202 of The National Security Act of 1947 (Title 10,Section 133, U.S. Code).

21. DOD Directive 5100.30.

22. Title 10, Section 133d, U.S. Code.

23. Section 202, National Security Act of 1947.

24. Title 50, Section 401, U.S. Code.

25. Title 10, Section 141d, U.S. Code.

26. Title 10, Section 142 and 143, U.S. Code.

27. Joint Chiefs of Staff, JCS Pub 2 (Washington, D.C., 1972).

28. Title 10, Sections 133d, 3034, 5081, and 8034, U.S. Code.

29. See "EMP" The Army Communicator, 14:5-10 (Spring 1979) for a discussion of EMP effects.

30. See SRI International, A Retrospective Look..., pp. 1-5.

31. See Dennis Bodson, EMP, Lightning, and Power Transients: Their Threat and Relevance (Washington, D.C., 1970).

32. "EMP," p. 8.

33. Michael King and Paul Fleming, "An Overview of the Effects of Nuclear Weapons on Communications Capabilities," Signal, 34:64 (January, 1980).

34. Bell Laboratories, EMP, Engineering and Design Principles (Whippany, N.J., 1975), p. 109.

35. King, p. 64.

36. Ibid.

37. Benjamin Schemmer, "Is C^3 America's Achilles Heel?", Armed Forces Journal International, 115:22 (September, 1979).

38. From testimony of DOD officials at "FY 1980 R & D Hearings," pp. 3391, 3396, 3399.

39. Wallace Henderson, "Surveillance and Warning," Signal, 33:39 (November/December, 1978).

40. Ibid.

41. Ibid.

42. Many of our important surveillance facilities are located in remote sites on the coasts of the United States and in Northern Canada. They become increasing vulnerable to conventional attack as the Soviets develop improved Precision Guided Munitions (PGM). Admiral Kaufman (Director of Command and Control in OJCS) described them in testimony as being "only as hard as a hand grenade." PGM's could be delivered by submarines or Backfire Bombers.

43. First Use of Nuclear Weapons, Hearings before the Subcommittee on International Security and Scientific Affairs of the Committee on International Relations, House. 94th Cong., 1st Sess. (Washington, D.C. 1976), p. 185. (Hereafter referred to as "First Use.")

44. Department of Defense, Department of Defense Annual Report for Fiscal Year 1975 (Washington, D.C., 1974), p. 38. (Hereafter referred to as Annual Report FY 75.)

45. Herman Kahn, On Escalation (New York, 1965), passim.

46. Department of Defense, Department of Defense Annual Report for FY 1981 (Washington, D.C. 1980), p. 66. (Hereafter referred to as Annual Report FY 1981.)

47. Herbert Scoville, "Flexible Madness," Foreign Policy, 22:23ff (Spring 1974).

48. "Annual Report FY 1980," p. 69.

49. James E. Dornan, et al., War Termination Concepts and Political, Economic and Military Targeting (Washington, D.C. 1978), p. 11 ff.

50. Schelling, p. 6.

51. Richard B. Foster, The Soviet Concept of National Entity Survival (Washington, D.C. 1978), pp. 41-42.

52. Ibid.

53. Adams, et al., p. 28.

54. Brodie, p. 222.

55. Committee on Armed Services, Senate, Hearings on DOD Authorization for FY 1980 Part 1, 96th Cong., 1st Sess. (Washington, D.C., 1979), p. 306.

56. Adams, et al., p. 28.

57. The Anti-Ballistic Missile Treaty.

58. Samuel Glasstone and Philip Dolan, Effects of Nuclear Weapons (Washington, D.C., 1977) (ERDA Bomb Calculator).

59. Given a CEP of 0.1 nautical mile and assuming the lethal radius equals the crater depth, one can use the equation provided by Schilling and Davis, ("Everything you wanted to know about MIRV and ICBM Calculations but Were Not Cleared to Ask," Journal of Conflict Resolution, June, 1979) which gives the Probability of Kill as $1-.5\ (LR/CEP)^2$. For one warhead the $P_k = .265$. If five warheads were used then $P_k = .79$ for a facility buried 400 feet underground. These are conservative P_k since the facility would be destroyed by overpressure before "dug up."

60. "First Use," p. 185.

61. From a draft paper American Telephone and Telegraph, Hardening and Survivability of the Telecommunications Network, an Overview, March, 1976.

62. Dornan, pp. 12-13.

63. "First Use," pp. 166 and 174.

64. Ibid., pp. 165-167. This possibility was raised by means of a footnote in a speech by Dr. Kissinger on February 3, 1976 before the Commonwealth Club of San Francisco.

65. "Launch on Warning" is not an official expression. It refers to launching a retaliatory strike after sensors reported it, but before the first impact. There are better options that do not require the U.S. to have a "hair trigger." For a discussion, see Richard Garwin, "Launch Under Attack to Redress Minuteman Vulnerability." International Security, 4:117-139 (Winter 1979/80).

66. Adams, et al., p. 38.

67. Ibid.

68. Ibid.

69. General Accounting Office, "The World Wide Command and Control System - Major Changes Needed in its ADP Management and Direction" (Washington, D.C., 1979), p. 3. (Hereafter referred to as "GAO WWMCCS Report.")

70. Ibid., pp. 2-6.

71. James Ray and Ted Schroeder, "The Revolution in Command and Control Technology and the Civilian -- Military Chain of Command" (Air Command and Staff College, 1977), p. 28.

72. George Rutter, "E-3A Enhancements," Signal, 110:11 (October, 1978).

73. "Annual Report FY 1980".

74. Henderson, p. 40.

75. "FY 1980 R & D Hearings," p. 3303.

76. "Watching the Action in Orbit," Time, 115:46 (March 24, 1979).

77. "FY 1980 R & D Hearings," p. 3293.

78. Schemmer, p. 25.

79. Ibid.

80. Ibid.

81. "FY 1980 R & D Hearings," p. 3326.

82. Ibid., p. 3304.

83. A. O. Sulzberger, Jr., "Error Alerts U.S. Forces to False Missile Attack," The New York Times, (November 11, 1979), p. 30.

84. Ibid.

85. "Doomsday Option," The Nation, 229:612-614 (December 29, 1979).

86. DOD Directive 5100.30, pp. 1-2.

87. Michael Putzel, "GAO: Pentagon Computer Crashes in Crisis," The Boston Globe (March 10, 1980), p. 3.

88. Ibid.

89. "GAO WWMCCS Report," ii ff.

90. Ibid.

91. "Computers and U.S. Military Don't Mix," Science, 207:1183 (March 14, 1980).

92. John Morgenstern, "Strategic and Tactical Command and Control System," Signal, 32:25 (November/December, 1978).

93. Ibid.

94. Ibid.

95. Richard Hartman, "Internetting and ADP Bolster Strategic C^3," Defense Electronics, 10:59 (September, 1979).

96. Adams, et al., p. 59.

97. Morgenstern, p. 16.

98. Comments by Ray Tate retired Deputy Director National Security Agency to KSG seminar.

99. "First Use," p. 215.

100. Ibid.

101. Ibid., p. 216.

102. Ibid., p. 215.

103. Morgenstern, p. 20.

104. "FY 1980 R & D Hearings," p. 3296.

105. Ibid.

106. Ibid., p. 3296.

107. Gorden Nagler, "Seafarer," Signal, 31:14 (January, 1977).

108. "FY 1980 R & D Hearings," p. 3296.

109. Ibid., p. 3289 ff.

110. Ibid., p. 3289.

111. Ibid., p. 3304.

112. "Annual Report FY 1980," p. 134.

BIBLIOGRAPHY

Books

Art, Robert and Kenneth Waltz. The Use of Force. Boston: Little, Brown and Co., 1971.

Brodie, Bernard. Strategy in the Missile Age. Princeton: Princeton University Press, 1971.

Glasstone, Samuel, and Philip Dolan. The Effects of Nuclear Weapons. 3rd ed. Washington, D.C.: U.S. Department of Defense, 1977.

Kahn, Herman. On Escalation. New York: Frederick A. Praeger, 1965.

Mallen, Lloyd. Peace is a Three-Edged Sword. Englewood Cliffs, N.J.: Prentice Hall, 1964.

Schelling, Thomas. Strategy of Conflict. New York: Harvard University Press, 1960.

_____. Arms and Influence, New Haven: Yale University Press, 1966.

Sokolovskii, V. D. Military Strategy, trans. Harriet Scott. 3rd ed. New York: Crane Russak & Co., 1974.

Tsipis, Kosta, Anne H. Cahn, and Bernard T. Feld. The Future of the Sea-Based Deterrent. Cambridge: MIT Press, 1973.

Newspapers and Periodicals

Black, Kent M. "TACAMO," Signal, 33:7-13 (September, 1978).

"Computers and U.S. Military Don't Mix," Science, 207:1183-1187 (March 14, 1980).

"Doomsday Option," The Nation, 229:671-677 (December 29, 1979).

Doubleday, Van C. "Expanding the Reins of Command," Signal, 31:42-46 (January, 1977).

"EMP," The Army Communicator, 14:5-10 (Spring 1979).

Fawcette, James. "C^3: Key Challenge Faces Military Planners," Electronic Warfare/Defense Electronics, 10:57-58 (June, 1978).

Hartman, Richard. "The Human Equation: C^3I's for People," Electronic Warfare/Defense Electronics, 10:61-64 (June, 1978).

_____. "Internetting and ADP Bolster Strategic C^3," Defense Electronics, 11:23-24 (September, 1979).

Henderson, Wallace D. "Surveillance and Warning," Signal, 33:39-43 (November/December, 1978).

Herzfeld, C. M. "Command, Control and Communications," Adelphi Paper, 145:40-43 (Spring, 1978).

James, Daniel. "C^4 in NORAD," Signal, 31:14-42 (September, 1977).

King, Michael, and Paul Fleming. "An Overview of the Effects of Nuclear Weapons on Communications Capabilities," Signal, 34:27-30 (January, 1980).

Kissinger, Henry A. "NATO: The Next Thirty Years," Speech delivered September 1, 1979 to NATO, Survival, 21:264-268 (November/December, 1979).

"Military Command and Control," Signal, 34:38-41 (January, 1980).

Morganstern, John. "Strategic and Theater Command and Control Systems," Signal, 32:46-48 (November/December, 1978).

Nagler, Gordon R. "Seafarer," Signal, 31:7-8 (January, 1977).

"Packet Switching Seen for Weapons Use," Aviation Week and Space Technology, 111:61-63 (September 17, 1979).

Putzel, Michael. "GAO: Pentagon Computer Crashes in Crisis," The Boston Globe (March 10, 1980), p. 3.

Rutter, George W. "E-3A Enhancements," Signal, 110:9-14 (October, 1978).

Schemmer, Benjamin. "Is C^3 America's Achilles Heel?", Armed Forces Journal International, 115:18-23, 28-30 (September, 1979).

Scoville, Herbert. "Flexible Madness," Foreign Policy, 22:22-31 (Spring, 1974).

"Seafarer Fund Drive Spurred by Navy," Aviation Week and Space Technology, 109:51-54 (April 4, 1977).

"Seafarer: NAS Sees No Basic Hazard," Science News, 112:101-2 (August 13, 1977).

Shriver, Richard H. "C^2 Planning for the Future," Signal 31:6 (March, 1977).

Stafford, Thomas P. "The Challenge of M-X," Signal, 33:8-12 (September, 1979).

Sulzberger, A.O. "Error Alerts U.S. Forces to False Missile Attack," The New York Times (November 11, 1979), p. 30.

"Watching the Action in Orbit," Time, 115:46-47 (March 24, 1979).

Government Publications

Bodsun, Dennis. EMP, Lightning, and Power Transcients: Their Threat and Relevance to EMP Protection Standards For Telecommunications Facilities, Technical Information Bulletin 78-1. National Communications System, 1978.

Department of Defense. Department of Defense Annual Report FY 1975. U.S. Government Printing Office, 1974.

_____. Department of Defense Annual Report FY 1980. U.S. Government Printing Office, 1979.

_____. Department of Defense Annual Report FY 1981. U.S. Government Printing Office, 1980.

_____. Department of Defense Directive 5100.30 Subject: Worldwide Command and Control System (WWMCCS). December 2, 1971.

_____. Department of Defense Directive 5137.1 Subject: Assistant Secretary of Defense (Communications, Command Control, and Intelligence). March 11, 1977.

General Accounting Office. The Worldwide Military Command and Control System - Major Changes Needed in its Automated Data Processing Management and Direction. December 14, 1979.

Office of Technology Assessment. The Effects of Nuclear War. Washington, D.C.: U.S. Government Printing Office, 1979.

Review of Defense Command, Control and Communications Systems and Facilities. Report by C^3 Panel to Committee on Armed Services. House. 94th Congress, 2nd Session. U.S. Government Printing Office, 1977.

"United States Intelligence Activities," Executive Order 12036. Federal Register 3674. January 24, 1978.

Hearings

Department of Defense Appropriations for FY 1979 Part 5: Research, Development, Test and Evaluation. Hearings before Committee on Appropriations. Senate. 95th Congress, 2nd Session, pp. 463-498.

Department of Defense Authorization for Appropriations for FY 1980 Part 6: Research and Development. Hearings before Committee on Armed Services. Senate. 96th Congress, 1st Session. April, 1979. pp. 3286-3404.

Department of Defense Authorization for Appropriations for FY 1980 Part 1: Defense Posture. Hearings before Committee on Armed Services. Senate. 96th Congress, 1st Session. January, 1979. pp. 298-411.

First Use of Nuclear Weapons: Perserving Responsible Control. Hearing before Subcommittee on International Security and Scientific Affairs of the Committee on International Relations House. 94th Congress, 2nd Session. March, 1976.

Hearings on the Military Posture Department of Defense Authorization for FY 1978. Part 3: Research and Development, Book 1 and 2, Committee on Armed Services. House. 95th Congress, 1st Session. pp. 642-668, 1844-1910.

Hearings on the Military Posture -- Department of Defense Authorization for FY 1980. Part 3: Research and Development, Book 1. Committee on Armed Services. House. 96th Congress, 1st Session. pp. 185-242, 1403-1461.

Hearings on the Military Posture -- Department of Defense Authorization for FY 1980. Part 4. Committee on Armed Services. House. 96th Congress, 1st Session. pp. 613-684.

Radiation, Health and Safety. Hearings before Committee on Commerce, Science and Transportation. Senate. 95th Congress, 1st Session. pp. 369-441.

Studies and Unpublished Papers

Adams, Robert B., "Command and Control Systems Evolution and Management in DOD," (Research Study, Army War College, National Technical Information Service, 1974).

Ames, Donald L. "Centralization: A Review and Analysis," (Professional Study, Air War College, National Technical Information Service, 1975).

Bowers, Bruce G. "Civilian Control of the Military: Historical Precedents for Today's Realities," (Research Report, Air War College, National Technical Information Service, 1978).

DeWilde, David A. "A Command and Control System for the NCA: What's Needed," (Professional Study, Air War College, National Technical Information Service, 1976).

Donovan, James E. et al. War Tremination Concepts and Political, Economic, and Military Targeting. SRI International, March, 1978.

Foster, Richard B. The Soviet Concept of National Entity Survival. SRI International, 1978.

Ray, James, and Ted Schroeder. "The Revolution in Command and Control Technology and the Civilian -- Military Chain of Command," (Research Study, Air Command and Staff College, May, 1977).

Stanford Research Institute. A Retrospective Look at Some of the Basic Issues Connected with National Command-Control and Communications, SRI International, Menlo Park, 1962.

2. THE STATUTORY BASIS FOR THE AUTHORITY OF THE NATIONAL COMMAND AUTHORITY

A Study of the Powers Vested in
the President and the Secretary of Defense
by the National Security Act of 1947 and Its Amendments

Newell Highsmith

TABLE OF CONTENTS

INTRODUCTION

The command structure of the U.S. military following World War II was not statutorily mandated. Orders were transmitted from the President, to the secretary of the department involved (Army or Navy), to the chief of the service, and finally to the executing commander. In addition, the exigencies of WWII had prompted the creation of unified commands composed of forces from both military departments (e.g., the European Command under General Eisenhower). When a unified command, rather than a single service, was to execute an order, the order would pass through the secretary and the chief of the department that was the executive agent of the unified command. One of the services was assigned executive agent duties when each unified command was created. The Joint Chiefs of Staff were, at that time, loosely organized with a staff consisting of numerous ad hoc committees. The chiefs divided their time as they chose between their duties as administrators of separate services and their duties as joint strategic planners within the Joint Chiefs of Staff.

Since 1958, the U.S. command structure has been governed by the National Security Act of 1947 as amended in 1949 and 1958. Under that structure, orders are given by the National Command Authority, which consists of the President and secretary of defense. The chain of command flows directly from the National Command Authority to the executing unified or specified commander with the Joint Chiefs of Staff playing a minimal role in the chain. The military department secretaries are not in the chain of command at all. In addition, the National Command Authority has the authority and has, on occasion, exercised the authority to transmit its orders directly to an executing officer or soldier. Organizationally, the military

departments are no longer separate executive departments, but are within the Department of Defense and under the direction of the secretary of defense. The Joint Chiefs of Staff have specific statutory duties and are supported by a staff that is set by statute at 400 officers.

These significant changes in the national command structure have come in stages, accompanied by legislative debate and executive advocacy. The purpose of this paper is to examine the changes and their rationales so as to reach an understanding of the statutory framework and determine whether (and how) further changes should be brought about.

THE NATIONAL SECURITY ACT OF 1947

The national security establishment has changed dramatically since the beginning of WWII, as the United States has had to evolve from comparative isolationism to global activism. Political and economic changes (an era of revolutionary nationalism, energy crises, recessions, etc.) have combined with technological advances to create a world situation that presents ever-changing challenges to the military and civilian authorities. In the wake of WWII, President Truman submitted to the Senate a proposed bill (S.758, 80th Congress) that was designed to provide a working framework for a number of reforms in the military establishment -- reforms that the war had shown to be necessary. The proposed bill had been drafted by "representatives of the armed services" and had been approved by the Secretary of War, the Secretary of the Navy, and the Joint Chiefs of Staff (the JCS).[1]

Prior to 1947, the Department of War and the Department of the Navy were totally separate executive departments. The JCS, a "loose structure of committees--some full-time, some part-time"[2]--had no statutory mandate,

and thus provided coordinated strategic guidance only as their duties as service chiefs allowed. No law compelled them to give strategic planning priority over administration of their respective services. Though WWII had forced the two branches to combine some of their forces under unified commands, no statute insured continuation of such arrangements or set up the apparatus for creating such arrangements. Since 1921, Congress had seen at least 60 bills introduced regarding unification of the military services. Jealous of their independence, the two military departments nonetheless recognized the need for increased unity and cooperation. In May 1946, the departments' differing views on "unification" were outlined in a letter to President Truman; and on June 15, 1946, Truman informed the department secretaries of his view on their points of disagreement in an effort to aid in their resolution. With this guidance, Secretary of War Robert Patterson and Secretary of the Navy James Forrestal hammered out their differences to produce a proposed bill that both services could support (S. 758).

Recommending passage of the bill as amended in committee, the Senate Committee on Armed Services expressed the intention of "bringing to the military departments in peacetime a large measure of the unity and commonness of purpose which characterize the operations of the armed services in time of war."[3] Fresh in mind were the lessons of a modern, global war that, although successfully concluded, had "disclosed certain fundamental weaknesses in our security structure" such as "our slow and costly mobilization, our limited intelligence of the designs and capacities of our enemies, our incomplete integration of political and military objectives, and finally, our prodigal use of resources."[4]

The National Security Act of 1947 resulted from Congressional action

of the President's proposed bill. The act's legislative history contains a lengthy discussion of overall objectives as well as specific provisions by the Senate Committee on Armed Services. Pervading this discussion is the committee's concern -- or its perceived need to respond to the traditional American concern -- over the prospect of maintaining a powerful standing army in peacetime. While recognizing the nation's emerging role in policing world peace, the committee suggested that unification should be an evolutionary process. The committee insisted that the act's cautious steps toward unification of the military services created a structure that "facilitates Presidential control of the armed forces, and enables Congress to examine and consider as a whole, rather than as unrelated pieces, the requirements and developments of the armed forces."[5] In short, the committee hoped to insure that "the traditional and fundamental principle of civilian control be not impaired."[6]

The chain of military command was changed little by the provisions of the act of 1947. The President's orders continued to pass through the full chain of military command with no provisions for bypassing unneeded links to reach the executing officer. Each command passed through the department secretary, the service chief, and only then to the unified commander (who in turn had to pass the order to the executing officer). The act did provide for: 1) policy guidance by a National Security Council; 2) mobilization policy guidance by a National Security Resources Board; 3) "general direction" of the national military establishment by a secretary of defense; and 4) unified strategic planning and direction by a statutorily mandated JCS.[7] (The act statutorily clarified the informal role of the JCS as the strategic and logistic planners for the national military establishment and as the

"principal professional military advisers" to the President and the newly created secretary of defense. It also provided for a joint staff to take over some of the functions of the loosely organized JCS committees.[8])

The secretary of defense (or SD) was named the "principal assistant to the President in all matters relating to the national security" (Section 202). Congress intended to "provide an individual with authority and responsibility who can be charged with and held accountable for the maintenance of the most effective security structure."[9] Yet grave and rigid restrictions on the secretary's authority prevented the fulfillment of those wide-sweeping duties. Under the terms of the act, the SD was hampered in five important ways. First, he could exercise only "general direction, authority, and control" over the military departments supposedly under his charge. The word "general" proved to be a critical qualification. Second, the Secretaries of the Army, the Navy, and the Air Force could go to the President or the Director of the Budget directly--over the head of the SD. Third, all powers and duties not granted explicitly in the act to the SD were reserved to the department secretaries--quite a limitation given the high level of generality in the statutory language. Fourth, the SD was explicitly denied authority over administration of matters that concerned only individual military departments. (In practice, virtually all functions that the services preferred to administer themselves were arguably of importance only to the one branch involved and were, therefore, guarded jealously by that branch.) Finally, the SD headed an executive department that was in no way superior to the three executive departments of the three services. Even though the SD was ostensibly the President's principal adviser, the military secretaries had equal footing on the various boards and councils. The SD

could be out-voted by the secretaries on the National Security Council, by-passed by the secretaries to reach the President, or simply roadblocked in his efforts to implement changes by chiefs and secretaries questioning his statutory authority.[10] The SD's attempts to implement programs administratively were subject to the cooperation of the services. Despite wasteful overlap, independent programs were effectively guarded because the SD could not back up his efforts with unequivocal statutory authority. The services argued that "general" authority allowed the SD to make general recommendations, but not to impose specific programs of reorganization. Thus, every move by the SD was clouded by uncertainty concerning the scope of his authority and the nature of his role in the national military establishment.

The SD was far from the position he would eventually hold as a component of the National Command Authority (or NCA, the ultimate military authority, consisting of the President and the SD). Congress, despite its lofty pronouncements of purpose in creating a secretary of defense, was as yet reluctant to vest full command over the military establishment in any one person other than the President. This concern over concentrating military authority in an appointed official was still an important factor in 1949, when the act was amended, and in 1958, when the Defense Department was reorganized.

In fact, Congress even looked upon unchecked Presidential power over the military as unwise, and consequently refused in 1958 to remove remaining statutory restrictions from the President.[11] Congress preserved its "prerogative of making the final determination as to the military needs and requirements of our nation,"[12] pursuant to Article I, Section 8 of the Constitution. (Section 8 imposes on Congress the duty to "...raise and support Armies" and to "provide and maintain a Navy.") Thus, the President had un-

fettered command authority as "Commander-in-Chief of the Army and Navy of the United States" (Article II, Section 2 of the Constitution), but not full authority over the composition and functions of the services. Congress, instead, statutorily prescribed the fundamental functions and administrative divisions of the armed services. Moreover, in 1947, it did not even delegate to the SD the command authority that did vest in the Executive; the SD had no place in the chain of command. Orders continued to go from the President, to the appropriate military secretary, to the service chief, to the unified commander, and then to the executing officer.

The act of 1947 did provide a "practical and workable basis for beginning the unification of the military services and for coordinating military policy with foreign and economic policy,"[13] and it moved slowly enough for the military establishement and its civilian control personnel to absorb the changes without undue turmoil. Clarification of a chain of command was not yet perceived as a problem, getting no attention in the act or its legislative history. Economy was the overriding concern, as it appeared "certain that military expenditures in the foreseeable future [would] necessarily be greater than in our former peacetime experience."[14] The primary command and control goal was to strengthen, but not necessarily streamline, the mechanism for "civilian control." Despite the cautiousness of the measures it enacted, Congress recognized that "the safeguard against militarism in this country is not to be found in the costly confusion and inefficiency of uncoordinated executive agencies with confused lines of authority. It abides rather in the solid conviction ... that the leaders of the armed forces are subordinate to their civilian heads, and through them to the President, the Congress, and the people."[15] The Senate Committee on Armed Services asserted

that stronger control by the Congress and the Chief Executive would be achieved by creating a unified military organization that could effectively be grappled with as a "single" entity. The act of 1947 paved the way for more extensive measures. As time passed and the steps already taken proved successful, Congress and the nation became more amenable to such measures.

THE 1949 AMENDMENTS

The act of 1947 was explicitly a reaction to the lessons learned in WWII. Thus, the assumptions underlying its structure were inextricably tied to the types of military preparedness deemed necessary in the aftermath of that war. The extremists who advocated total unification of the military services were defeated by the guarded independence of the Army and the Navy, by their scheme's similarity to the German and Japanese military systems in WWII, and by American aversion to any monolithic military machine. The act of 1947, therefore, attempted to begin the thawing of the rigidly frozen structure to allow for organic change.

But little attention was paid to the command structure and no streamlining measures were enacted. Warfare was conceived of an a grand scale, in which the military chain of command, rigid and diffuse as it was, played a much-needed role. In a global war, like WWII, the President would have no business directing a particular force in a particular area; his job is too demanding to allow attention to such minutiae. Only when the perspective shifts away from an "all-out war" scenario do we encounter a need for the NCA to direct a politically sensitive, but limited operation--for example, in Cuba or Iran. Moreover, in 1947, direct command of forces in the field by the President or the SD was not yet possible technically. So a flexible

statutory structure governing the chain of command was neither a perceived nor a real need. And the act had reformed the non-integrated chain of command somewhat by giving statutory validation to the unified overseas commands that were established under the duress of WWII.

In 1949, the U.S. Commission on Organization of the Executive Branch of the Government (the Hoover Commission, chaired by former President Herbert Hoover) disclosed its findings in a report that prompted much debate and some action. The report made recommendations for reorganization of virtually every department in the executive branch, and found that "the National Military Establishment as set up in the act of 1947 is perilously close to the weakest type of department."[16] The chief reason was that statutory authority was delegated to subordinate units--i.e., the military departments--while the department head had only "general" supervisory powers. The individual who was responsible and accountable to the President, the SD, lacked authority to exercise control over the organization under his charge. Under the act, a "rigid statutory structure" was established that prevented the SD from providing unified direction of the military branches, and thus undermined firm civilian control of the armed forces by the President.[17]

President Truman responded to the Hoover Commission Report by recommending that Congress amend the act of 1947 to create a Department of Defense (DOD) as an Executive Department, with the Army, Navy, and Air Force as component military departments and with full authority over the military establishment vested in the SD. Truman's March 5th message to Congress reflected a changing strategic outlook:

> The development of man's ability to shrink space and time and to control natural forces makes imperative a corresponding development of the means for directing and controlling these new powers.[18]

Though Truman spoke of future, ongoing command and control problems in a technologically dynamic world, Congress continued to speak in terms of the "lessons of WWII"--one of which was the evil of militarism. The broader lesson of the need for unflagging attention to the problem of strategic preparedness in a fast-changing world tended to be subordinated to narrow lessons of strategy that were specifically geared to WWII-type threats--lessons that often failed to apply in the advancing nuclear age. The amendments' legislative history and the Armed Services Committees' hearings reveal a primary concern for economy, efficiency, and firm civilian control, again with little explicit attention to command and control problems. Nonetheless, changes were made in the statutory command structure.

The 1949 amendment process began with President Truman's recommendations of March 5th, following publication of the Hoover Commission Report. The Senate responded with a bill that largely adopted those recommendations (S. 1843, 81st Congress), but the House acted on a bill that dealt solely with the budgeting process of the military (H.R. 5632). To insure that his proposals would be voted on by all members of Congress even if a bill did not emerge by the normal legislative process, Truman submitted Reorganization Plan No. 8 of 1949, which instituted as many of his recommendations as could be enacted by reorganization plan.[19] Whether prompted by the President's persistence and sense of urgency or not, the Senate amended H.R. 5632 by replacing all but the enacting clause with the text of S. 1843. The conference between the managers of the bill in the House and the Senate resulted in the final wording of the 1949 amendments. This version paralleled the more comprehensive Senate bill, addressing most of the issues raised by the President.

The Congress clearly saw the 1949 amendments as just another step in the ongoing process of organizational evolution. No final statutory framework was intended or expected. Rather, the Senate Committee on Armed Forces noted that "there is considerable criticism that the proposed legislation is somewhat too conservative.... The Committee feels that the measures recommended in the legislation are fully adequate at the present time [emphasis added] and do not go beyond correcting the weaknesses which 18 months of experience has clearly shown to exist in the 1947 Act."[20] The amendments were perceived as part of a process, not a final system. One lesson of WWII, that of vigilance to detect and meet the constantly changing national security needs of our country, was clearly on the minds of the decision makers in 1949. The amendments themselves and the process by which they were constructed show a legislative intent to make national security reform an ongoing task.

In hearings on the proposed amendments, then Secretary of Defense James Forrestal said that:

> ...the authority of the Secretary of Defense has proved to be circumscribed to a point where it has not been possible for him to assume his full responsibilities as the principal assistant to the President in all matters relating to the national security.[21]

Forrestal identified as a prime culprit the 1947 provision reserving to the military secretaries all authority not specifically assigned to the SD--which in practice meant all but supervisory authority at the most general level. The 1949 amendments eliminated that provision entirely, and in addition: 1) made the Department of Defense an executive department, with the three branches comprising military departments within, and subordinate to, the DOD; 2) gave the SD the authority of an executive department head; 3) deleted the word "general" in describing the SD's power, authority, and duties; 4) gave the SD alone a seat on the National Security Council; and

5) barred the military secretaries from going over the head of the SD to the President or the director of the budget. (Congress did leave to each secretary and service chief the authority to present to Congress, after notifying the SD, "any recommendation relating to the Department of Defense that he may deem proper."[22] The Senate bill would allow such action only upon request by Congress, but the conference version specifically allowed access on the initiative of the individual secretaries and chiefs. Nonetheless, the organization of the executive branch itself was modified to prevent circumvention of the chain of authority. Congress insured both the non-insularity of the secretaries' and chiefs' views and independent channel of information--information essential for maintaining a viable role in national security policy-making.)

Although ultimate authority was vested in the President and the SD, as with the present-day NCA, Congress still resisted concentrating unimpaired authority over the structure and functions of the military establishment. Much of the rhetoric used in the hearings and the legislative history was that of "civilian control," but the thrust of the Congressmen's questions and the substance of their differences with the Truman Administration pointed to a slightly different concern--that of concentration of authority over the military. In fact, Secretary Forrestal felt constrained to head off such objections at the outset:

> I would like to address myself briefly to what I believe may be the chief objection raised to the proposed amendments: namely, that these amendments would vest in the Secretary of Defense too great a concentration of power emphasis added . I have given long and serious thought to this obje tion because it is similar to an objection to which I lent my support 2 years ago.... I must admit to you quite frankly that my position on the question has changed.... There are adequate checks and balances inherent in our governmental structure to prevent misuse of the broad authority which I feel must be vested in the Secretary of Defense.[23]

Despite this assertion, Forrestal still faced pointed questions, particularly from Senator Lyndon Johnson, and could not help but admit that the changes the President sought would result in significant concentration of power and some inherent risk.[24] Even though the President sought increased efficiency and accountability in the executive branch, Congress was not willing to vest unfettered administrative authority in the SD. Forrestal argued that the proposals "would place no powers in the Secretary of Defense which are not already vested in the President,"[25] and that consequently, Congress need not fear radical changes in the service system from any "new" concentration of authority. Yet such changes seemed to be precisely what Congress feared, for it amended the President's proposals to insure the inviolability of the services.

The SD remained hindered by statutory restrictions. Though his authority was significantly increased, the SD still suffered restrictions on his power to reassign, transfer, abolish, or consolidate military functions. He could not tamper with the statutorily designated "combatant functions" of the three services. And more importantly, the amendments stated that the military departments to be "separately administered by their respective secretaries,"[26] which led to constant squabbling over where to draw lines of administrative authority between the DOD and the services. (Congress did not explain the contradiction between a unified executive department and internally fragmented administrative responsibilities.)

Just as Congress moved cautiously in extending authority to the SD, it refused to grant the newly created chairman of the JCS the broad duties requested by the President. The House and Senate were unwilling to make the chairman the "principal military adviser" to the President, preferring to

assign that duty to the JCS as a whole.[27] In the hearings, the committeemen were concerned that access to the President by only one person would dangerously concentrate power because the airing of dissident views would not be assured. The chairman might acquire a disproportionate influence on the professional opinions reaching the President.

The concern over concentration of power is apparent from the questions asked by Congressmen in hearings on the bill, from the administration's efforts to ease any such concern (even prior to its being expressed), and more importantly, from the kinds of restrictions imposed in 1949. These restrictions, on the surface, presented no command and control problems; the chain of command could be altered as the President chose, for his command authority was unimpaired. (In fact, President Eisenhower did change the chain of command prior to 1958, and Congress noted his Constitutional authority to do so in the legislative history accompanying the 1958 Reorganization Act.) However, the limitations did affect the ability of the SD--and consequently the President--to organize the department they so freely commanded. The efficiency and economy of civilian command and control was inevitably affected by the NCA's inability to administer the DOD as a unit so as to eliminate wasteful overlap and non-uniformity. In the area of weapons development and procurement, for example, overlap and non-cooperation tended to breed service rivalry, increased cost, and systems that would not interface effectively (problems we face today).

The statutory restrictions in the 1949 amendments did insure the independence of the services and their respective functions. But, according to the administration, they also created ambiguity and uncertainty regarding the SD's authority, and rendered the SD incapable of administering the

department even to the extent Congress intended.[28]

Why did Congress allow inefficiency and wastefulness in order to avoid concentrated authority that might eviscerate the independent services? Does the service system provide diffusion of authority so as to prevent militarism or oppression by the Executive? Surely not. Congress noted in 1947, as others have since, that democratic principles--such as separation of powers and the sovereignty of the people--are the true guards against militarism in this country.[29] The hearings and the legislative history are devoid of any suggestions that the national security is enhanced by the limitations on the SD's authority to administer the DOD. Congress does have a constitutional duty to provide for an Army and a Navy, but the broad language of Article I, Section 8 gives Congress great leeway to be activist, deferential, or anything in between. So whatever its rhetorical value, this constitutional duty does little to explain why Congress acted to preserve a service system as opposed to other possible courses of action.

One possible answer to why Congress has refused to extend full administrative authority is the influence of pro-service system special interests. Individuals with jealously guarded spheres of authority, industries that benefit from the proliferation of projects and services, and any number of other vested interests undoubtedly influence the decision makers, but it is difficult to gauge their impact beneath the "checks-and-balances" rhetoric. What <u>can</u> be said is that the task facing a Chief Executive who wants further authority to reassign, transfer, abolish, or consolidate functions is threefold: 1) prepare to meet concentration-of-power rhetoric at a rhetorical level; 2) identify and try to counteract the lobbying interests that will be influencing the Armed Services Committees; and 3) impress upon

Congress the magnitude of the burden--both fiscally and in terms of effectiveness--that is caused by overlapping, non-interfacing functions. Much of the opposition to such measures will not come as testimony before a committee, but will work its influence more subtly. That is precisely what the Eisenhower Administration faced in 1958 when it vigorously campaigned for reorganization of the DOD.

THE DEPARTMENT OF DEFENSE REORGANIZATION ACT OF 1958

In 1958, the debate over DOD reform involved the same issues as in 1949; however, the call for change was more insistent and no longer based on the now-obsolete strategic scenario of WWII. Legislative action was deemed necessary to keep the department abreast of new, ever-changing national security threats. As President Eisenhower said:

> Thermonuclear weapons, missiles, new aircraft of great speed and range, atomic ground weapons, nuclear submarines have changed the whole scale and tempo of military destructiveness. Warning times are vanishing. There can be little confidence that we would surely know of an attack before it is launched. Speeds of flight are alrealy such as to make timely reaction difficult and interception uncertain.[30]

Congress, at the President's urging, reassessed the statutory framework of the defense system. It was recognized that "the products of modern technology are not, in many cases, readily adaptable to traditional service patterns or existing provisions of law."[31] The question for Congress, then, was how to balance the President's requested reforms against its apparent aversion to concentrated authority and its desire to maintain the separateness of the services.

Appearing before the House Committee on Armed Services in support of the President's recommended reforms, Secretary of Defense Neil McElroy echoed

Eisenhower in describing the new threats, and added that the 1947 act as amended did indeed "suit our military needs as they could be seen at the time."[32] But times had changed and so must the statute. He emphasized the heightened need for clearer lines of command and for the pre-eminence of unified commands over the traditional services. As Eisenhower states to Congress, "The unified commands...are the cutting edge of our military machine....Our entire defense organization exists to make them effective."[33] The committee members in the House and the Senate, however, parried these arguments with questions about concentrating power and emasculating the services as viable, separate entities. In the end, the legislative process again brought a compromise--one that rejected total flexibility and efficiency-mindedness for residual statutory barriers and restrictions.

The military chain of command, fully under the authority of the Commander-in-Chief, had been modified by the SD prior to consideration of the Reorganization Act, at Eisenhower's direction. In the legislative history accompanying the act of 1958, Congress noted that SD's action and said that "the changes contemplated in the chain of command can be accomplished without any change in law."[34] The executive agent system, by which the service with primary responsibility for a unified command served as executive agent, with orders passing through the secretary and the chief of that service, was discontinued as a command structure. The old system, which Eisenhower described as "cumbersome and unreliable in time of peace and not usable in time of war,"[35] was replaced by a system whereby the "chain of command [flowed] from the President to the Secretary of Defense to the unified commander."[36] Without the executive agent system, the role of individual service chiefs in the chain was significantly curtailed. Service chiefs no longer acted

as executive agents, but the JCS as a whole was directed to "furnish the advice and guidance upon which the orders of the Secretary of Defense are transmitted to unified commanders."[37] Prior to 1958, the JCS had not been "charged with operational responsibility," so the statutory limit on its staff was raised from 210 to 400 to allow it to "provide strategic direction of unified commands."[38]

The effort, as stated in the Congressional declaration of purpose, "to provide for the establishment of unified or specified combatant commands, and a clear and direct line of command to such commands" was to a large degree successful.[39] Section 202(j) of the 1947 act was amended to authorize the President, "through the Secretary of Defense and with the advice and assistance of the Joint Chiefs of Staff,"[40] to establish unified or specified commands. More importantly, combatant commands were made responsible solely to the President and the SD for "such military missions as may be assigned to them."[41] As a result, the service departments could no longer unilaterally take forces out of a unified command. And to further insure the inviolability of the unified commands, the service secretaries and chiefs were statutorily directed to supervise their departments "in a manner consistent with the full operational command vested in unified or specified combat commanders pursuant to Section 202(j)..."[42] However, although the services lost operational control and the authority to affect force structures, they retained administrative control over the forces in the unified commands--i.e., control over training, personnel management, logistics, etc. (The SD, though, could assign responsibility for support functions to any one or more services with forces in a particular unified command.) Further assurance that the military departments would not lose their separate identities was

provided by restricting the President and SD to the establishment of combatant commands. This provision prevented administrative functions from being organized into unified commands--such as a single command for all military training--which would have reduced the military departments to veritable shells.[43] Thus, the full subordination of the services to the unified commands, as sought by the NCA, was not achieved by the statute. Congress would not give the NCA the total flexibility it desired, despite the President's opposition to any restrictive provisions.

The Eisenhower administration denounced the provision in the 1949 amendments that the military departments should be "separately administered by their respective Secretaries" within the DOD. This language had produced endless battles over where to draw the line between separate administration and overall DOD administration by the SD. Again, however, Congress refused to fully comply with Eisenhower's request to "remove any possible obstacles to the full unity of our commands and the full command over them by unified commanders."[44] Instead, it changed the wording to make each military department "separately organized [emphasis added] under its own Secretary,"[45] thus refusing to eliminate all of the statutory barriers to NCA authority. No matter how persistently the administration asserted that it had "no desire to emasculate any of the four services,"[46] Congress was driven by its intention to statutorily protect the independence of the services.

Congress also used the 1958 act to bar the reassignment, transfer, abolition, or consolidation of any "function, power, or duty" vested in an agency by law unless a detailed report is submitted to the Armed Services Committess and neither House adopts a resolution blocking the change.[47] This provision was specifically designed to protect the traditional, sta-

tutorily mandated combatant functions of the respective military departments as described in 10 U.S.C. Sections 3062(b), 5012(a), 5013(a), and 8062(c)--for the Army, Navy, Marines, and Air Force respectively. (The statutory definition of the Army's combatant function is in broad terms and is similar to the definitions of the other services' combatant functions. Section 3062(b) of Title 10 reads: "In general, the Army, within the Department of the Army includes land combat and service forces and such aviation and water transport as may be organic therein. It shall be organized, trained, and equipped primarily for prompt and sustained combat incident to operations on land [emphasis added]. It is responsible for the preparation of land forces necessary for the effective prosecution of war except as otherwise assigned and, in accordance with integrated joint mobilization plans, for the expansion of the peacetime components of the Army to meet the needs of war." Eisenhower called for an end to the "doubts concerning the Secretary's authority to transfer, reassign, abolish, or consolidate functions of the [Defense] Department" and urged Congress to "be done with prescribing controversy by law."[48] But Congress again chose to provide checks and barriers to the secretary's authority, albeit through foreseeable jurisdictional controversy.

In short, the Reorganization Act of 1958, which completes the statutory framework still intact in 1980, fell short of the full flexibility--and unfettered authority--sought by the President and the SD. Authority over the establishment, operations, and support of unified and specified commands was offset by the vesting of administrative authority in the military departments. The streamlined chain of command no longer passed through department secretaries, but the secretaries retained "separately organized" departments.

The openings for subordination of the services' independence by the President or the SD were effectively blocked by the restrictions on changes in "functions" and the limitation of unified and specified commands to "combatant" or "military" missions.

CONGRESSIONAL INTENT (Summary)

Several themes dominate Congressional action regarding the military establishment. Immediate post-WWII attitudes tended to emphasize civilian control--not surprising, considering the immense military machine that was left after the war. Unification was justified largely in terms of strengthening civilian control, but was animated largely by economic considerations. The nation had been economically deprived for too many years, and it hoped to minimize the burden that maintaining a large peacetime force would inevitably bring. Economy and efficiency have been powerful factors in Congressional decisions and must not be ignored. However, the focus here must be on the command and control questions that motivated Congress.

In 1949, civilian control was again a key theme. But, as in 1947, the legislative history also suggested another theme that concerned Congress: concentration of military authority. At each stage of the legislative process that amended the act of 1947, Congress struggled with the President over specific language and numerous restrictions. The rhetoric of civilian control laced the legislative history; but in committee hearings, administration representatives faced repeated questions concerning concentration of power in civilian officials.

Congressional action to insure maintenance of a legitimate multi-service system has been the final compromise in the dispute between the Executive and

the Congress. In 1958, President Eisenhower saw the problem largely as one of clinging to outmoded, but statutorily mandated "service systems of an era that is no more."[49] Proponents of broad civilian authority in the Executive had to address objections that unfettered authority would lead to abolition of a service through transfer of a key function. Separation, protection of combatant roles, and protection of certain other functions such as training and personnel administration have been explicit goals of Congress, either because of powerful military special interests, attachment to traditional service concepts, fear of concentrated authority, or all three.

Of course, efficiency and flexibility have also beeen important Congressional goals. The Armed Services Committees, in particular, were quite responsive to Presidential requests, and complied with those requests with comprehensive legislation. Streamlining and thawing of awkward, rigid lines of command were markedly improved in 1949 and 1958. In short, Congress did not take lightly the need for an improved statutory structure for the military establishment; it merely balanced that need against other considerations. And although Congress eventually granted most of the desired reforms, much is learned from the reforms it did not grant--particularly when those reforms were vigorously endorsed by the President. In the legislative history, Congress said:

> . . . the provisions agreed to with respect to combatant functions recognizes the responsibility of the Congress as provided in the Constitution of the United States. It preserves to the Congress its prerogative of making the final determination as to the military needs and requirements of our nation.[50]

Congress, then, was not unmindful of strategic needs in the area of national security, but pursued its duties in assessing needs and capabilities in light of democratic principles.

CONCLUSIONS

Many of the problems that prompted Congressional action in 1947, 1949, and 1958 are very much alive today. There is still a need to reduce the troubling "tendency toward service rivalry and controversy";[51] to eliminate overlap and duplication in military services, functions, and weapon development (and to streamline chains of command and authority). These needs require unification and centralization, which can be achieved only be removing the statutory restrictions from the SD and the President so they will have the flexibility to speedily effect reforms as called for by the changing military/political/economic scene. The act of 1947 as amended has recognized the Executive's full authority over operational command. In practice, the only limitation on the NCA's authority to direct operations is its physical (technological) ability to communicate with the executing commander--or the executing soldier if necessary. Such flexibility has been a requisite of the nuclear era; even in 1958, it was acknowledged as necessary, given the need for split-second decision-making in politically-charged situations. Clearly, Congress was (and is) too slow to react in such situations, and military commanders cannot, in our democratic system, make decisions of such a political, "ultimate" nature.

The 1958 statutory structure gave sufficient flexibility in structuring military forces to react to WWII-type threats (through unified commands) as well as to threats in a Mutual Assured Destruction (MAD) strategic scenario (through the SIOP and some of the specified commands). However, that structure may no longer be preferrable from a strictly strategic point of view. In the wake of Vietnam, Iran, and Afghanistan, it is difficult to predict exactly what strategic challenge will next test our national security.

The political and economic volatility of the modern world is such that even the intelligence community has trouble anticipating where--and in what form--the next threat will develop. The military establishment, mired in bureaucratic sluggishness and service rivalry, lacks the "unity and commonness of purpose"[52] to adapt to the endless variety of threats it may be faced with. It may well be that the time has come for what President Eisenhower sought in 1958--total subordination of the services to the operational commands. The authority to "transfer, reassign, abolish, and consolidate" functions may be needed in any part of the world and may range from supplying food and medicine to full-scale military involvement. Under present law, the President can change the services' major functions only under imminent threat of hostilities.[53] But it is unclear whether the 1958 reference to "hostilities" would encompass situations that were not foreseen in 1958--limited crises such as in Iran or Afghanistan. And in any event, localized, non-global crises must be reacted to quickly. There is not time <u>after</u> hostilities threaten to make a post-hoc determination of authority and only then attempt to integrate forces and interface systems to meet the situation. Flexible capabilities must be pre-existing.

Should the recent, more hawkish view of our national security needs continue, it will be imperative that Congress reassess the 22-year-old statutory framework to insure that the NCA has sufficient authority to provide for the defense of this country. Many questions will need answering. Is the present statutory structure indeed outmoded, like that which existed prior to WWII? If it is, what factors deserve weight in the legislative process both for and against removal of statutory limitations? Does the desire to preserve a multi-service system outweigh strictly strategic

needs, warranting retention of statutory barriers?

Two points must be kept in mind in dealing with prospective reforms. First, past efforts have always been initiated by the Chief Executive and have been accompanied by vigorous campaigns to educate the nation and persuade the Congress. Therefore, both now and in the future, the executive branch must detect and request needed changes in the statutory structure, for it alone has the working knowledge necessary to do so. Congress is reactive in this area, not assertive. Second, Congress and the Executive have emphasized in each year--1947, 1949, and 1958--that the process of evaluation and reform of the military is an evolutionary process, and must continue to be so if it is to incorporate changing strategic outlooks. In 1949, Congress noted that students of the problem "have felt that the process is basically one of evolution" and "are in general agreement that the National Security Act of 1947 represented but a starting point and that it would be necessary to return to the act from time to time so as to reexamine its provisions in the light of experience."[54]

The supposedly ongoing task of reexamining the act for needed statutory changes has produced no amendments since 1958. Twenty-two years later, the same statutory structure governs the U.S. military establishment. Perhaps the pervasive preoccupation with "muscle" has led Congress and various Presidents to perceive no needed reforms because the technological threat--missiles, nuclear devices, satellites, etc.--has changed little (though refinement has been marked). President Eisenhower was stirred to action in 1958 by a change in the physical threat, a change in the type of muscle due to advances in nuclear and jet-engine technology. However, one long-neglected "lesson of WWII" is that new strategic threats to national security

come from political and economic shifts, not just shifts in military technology. A national security system that is set up by statute to respond to the most current "muscle" may be unable to respond to varying strategic applications of that muscle--applications guided by political and economic exigencies wholly unforeseen when the statute was written.

In a post-Iran, post-Afghanistan world, it may well be necessary, as noted earlier, to remove statutory restrictions on the SD and the President. Economic considerations demand elimination of overlap and duplication; strategic considerations militate against functions and systems that do not coordinate or interface effectively. An executive desirous of such changes will have to initiate reform and meet objections at the rhetorical level and in the lobbies of Congress. The apparent deterioration in the present world situation may provide the ammunition needed to shatter the remaining restrictions, for the Executive must impress upon Congress the seriousness and urgency of its proposals (as it did after WWII and during the Cold War). Only through a well-coordinated campaign can the Executive overcome Congressional inertia and force Congress to carefully reconsider its justifications for restricting the NCA. Upon reconsideration, Congress may adhere to its policy of restricting executive discretion in the management of military power--a policy evidenced by the War Powers Act. However, unreflecting adherence to a policy of restrictiveness would be a mistake, for the restrictions embodied in the National Security Act are fundamentally different from those in the War Powers Act. The War Powers Act proscribes the use of military force in sensitive situations in deference to Congress's explicit and exclusive Constitutional power to declare war. Conversely, the National Security Act limits the Executive's ability to <u>structure</u> the military

establishment and thereby insure national military preparedness. Congress's constitutional duty to "provide for an Army and a Navy" is less explicit and exact than its exclusive duty to declare war. Thus, de facto declarations of war by the Executive implicate more compelling constitutional issues than do even the most radical steps involving military preparedness. Moreover, the Executive can argue that the War Powers Act has itself proven too cumbersome, given the secrecy that was absolutely required during the 1980 effort to rescue the hostages in Iran. While members of Congress chose to brush aside charges that President Carter violated the act, the incident highlighted the act's inadequacies in the face of "unusual" threats--threats of the kind that can only be expected to recur in the future. The same argument may be extended to the statutory rigidity in the National Security Act. The legitimate concern in Congress over "undeclared wars" and irresponsible realignment of the military establishment might be better served by other methods of oversight than statutory restrictions such as the War Powers Act and certain provisions of the National Security Act.

It is easier to say "let us put partisan politics aside" than it is to bring it about. Yet, whatever the outcome, Congress must confront its reasons for maintaining the 22-year-old statutory structure of the DOD, and it must confront them in a straightforward manner. In these times of political instability, the nation deserves an unequivocal declaration of policy that explains both the changes made and the changes foregone.

NOTES

1. 1947 U.S. Code Congressional and Administrative News 1487. Report of the Senate Committee on the Armed Services. (Hereafter, 1947 U.S.C.C.&A. News).

2. Ibid., p. 1498.

3. Ibid., p. 1489.

4. Ibid., p. 1488.

5. Ibid., p. 1500.

6. Ibid.

7. See text of National Security Act of 1947, 1947, U.S.C.C.&A. News 499.

8. 1947 U.S.C.C.&A. News 1487, p. 1498.

9. Ibid., p. 1501.

10. See U.S. Commission on Organization of the Executive Branch of the Government (1947-1949). The Hoover Commission.

11. See Department of Defense Reorganization Act of 1958, 1958 U.S.C.C.&A. News 592.

12. 1958 U.S.C.C.&A. News 3281, 3285. Conference report on Department of Defense Reorganization Act of 1958.

13. 1949 U.S.C.C.&A. News 2488. President Truman's March 5th special message to Congress concerning "Unification of Armed Services."

14. 1947 U.S.C.C.&A. News 1487, 1489.

15. Ibid., p. 1500.

16. U.S. Commission on Organization of the Executive Branch of the Government (1947-1949), p. 189.

17. Ibid., p. 187.

18. 1949 U.S.C.C.&A. News 2488.

19. Pursuant to the Reorganization Act of 1949, the President could submit plans to Congress for improved organization of the executive branch. The national military establishment could not be as broadly reformed by such a plan as by Congressional action, but Truman used the plan at least in part to emphasize to Congress the importance he placed on reforming the national security system.

20. 1949 U.S.C.C.&A. News 1771, 1775. Report of the Senate Committee on Armed Services.

21. U.S. Congress. Senate. Committee on Armed Services. Volume 3. Hearings on the proposed amendments to the Act of 1947.

22. 1949 U.S.C.C.&A. News 590, 593. National Security Act Amendments of 1949.

23. U.S. Congress. Senate. Committee on Armed Services. Volume 3. Hearings on the 1943 amendments to the Act of 1947, p. 9.

24. Ibid., p. 22.

25. Ibid., p. 9.

26. 1949 U.S.C.C.&A. News 590, 592. See also, U.S. Congress. Senate. Committee on Armed Services. Volume 19. Hearings on Department of Defense Reorganization Act of 1958.

27. 1949 U.S.C.C.&A. News 590, 593.

28. 1958 U.S.C.C.&A. News 5432, 5433. President Eisenhower's April 3rd message to Congress. "Reorganization of the Department of Defense."

29. 1947 U.S.C.C.&A. News 1487, 1500.

30. 1958 U.S.C.C.&A. News 5432, 5433.

31. Ibid., p. 5433.

32. U.S. Congress. House. Committee on Armed Services. Volume 21. Hearings on H.R. 12541.

33. 1958 U.S.C.C.&A. News 5432, 5435.

34. 1958 U.S.C.C.&A. News 3272, 3276. Senate report on Department of Defense Reorganization Act of 1958.

35. 1958 U.S.C.C.&A. News 5432, 5436.

36. See 1958 U.S.C.C.&A. News 3272, 3276.

37. Ibid.

38. Ibid.

39. 1958 U.S.C.C.&A. News 592. Text of Department of Defense Reorganization Act of 1958.

40. Ibid., p. 597.

41. Ibid., p. 595.

42. Ibid., p. 595.

43. 1958 U.S.C.C.&A. News 3272, 3274.

44. 1958 U.S.C.C.&A. News 5432, 5436.

45. 50 U.S.C. Sec. 401.

46. U.S. Congress. Senate. Committee on Armed Services. Volume 19. Testimony of Secretary of Defense Neil McElroy in support of President's proposed reorganization.

47. 10 U.S.C. Sec. 125.

48. 1958 U.S.C.C.&A. News 5432, 5440.

49. 1958 U.S.C.C.&A. News 5432, 5434.

50. 1958 U.S.C.C.&A. News 3281, 3285. (See note 12.)

51. 1958 U.S.C.C.&A. News 5432.

52. 1947 U.S.C.C.&A. News 1487, 1489.

53. 1958 U.S.C.C.&A. News 592, 594.

54. 1949 U.S.C.C.&A. News 1771, 1773.

3. CONTROL OF SENSITIVE INFORMATION

Kenneth Freeman

TABLE OF CONTENTS

INTRODUCTION

The intelligence process is the gathering of raw information, its analysis, and then its presentation to the policy-making community. This process implies several dilemmas. In order for the intelligence community to be effective the information gathered must be digested and dispersed to the decision makers. But, in order for there to be confidential information, sources and methods must be protected. For a reliable evaluation of the data to be made, promising leads need to be pursued appropriately. But the citizen's constitutional rights must be protected; the constitution, the laws, and executive orders must be obeyed. Wide dispersal of information, at least in a sanitized form, to those who can benefit from it is tactically desirable. But there can be real strategic advantages to withholding information from those who can benefit from it.

Secrecy can be a cloak to protect legitimate sources and operations, to garner power, or a cloak to hide badly thought out plans, poor analysis, and incompetence from a more searching scrutiny.

A changing world has brought these issues into sharper focus. By the end of the American Civil War, the United States had reached a point where, because of its size, resources, and distance from potential competitors, it could afford to ignore its potential enemies in fact as well as in rhetoric. By the end of World War I this state of blissful non-involvement had begun to fade. Nevertheless, the United States at the end of World War II faced a confused world with unmatched resources, freedom of action and self-confidence.

The late sixties and the seventies have seen a change in the United States position. While still unmatched in resources and capability, the

U.S. no longer bestrides the globe like a colossus. Dependent upon foreign oil (and other resources) and with declining relative power vis à vis both its allies and the Soviet Union, it faces a world undergoing rapid social, economic, and political change.

In such an environment it has become increasingly important for the U.S. to understand cultures, political forces, and economic issues it had in the past been able to ignore. This quest for understanding requires that information be made available to as wide an audience as possible.

At the same time the spectacular post-war growth of the intelligence community, coupled with the revelation of abuses, dramatically increased the perceived need of Congress to exercise its constitutional role of overseeing the executive branch's conduct of intelligence. The need to keep Congress properly informed has substantially increased the number of people with access to an overall, as opposed to, an organizational perspective. This involvement of hitherto peripheral centers of knowledge and oversight, some with the legal authority to demand access to any relevant material, has heightened the tensions inherent in the control of information.

This paper focuses on how the widest possible dissemination of information interacts with the claims of secrecy to protect sources and methods, and with the withholding of information for strategic advantages and for bureaucratic or personal interest. It examines a series of incidents in which the issue of secrecy was highlighted. With one exception, the Bay of Pigs, the incidents are drawn from the ample documentation which has become available from World War II. This has the advantage of providing incidents whereby it is possible to gain at least a limited appreciation of the real stakes in lives, power, and confidentiality. It does suffer

from the weakness of being rooted in the distant past. It is, however, my belief that although times have changed, the underlying problems have not. Thus an examination of how the issue of confidentiality was handled in these instances is useful. The incidents chosen reflect confidentiality to protect sources, for strategic advantage, and for bureaucratic power.

Bureaucratic Power

Two examples have been chosen to illustrate how the withholding of information can be used to gain bureaucratic power. These are the Bay of Pigs and the control of the German nuclear weapons information in Great Britain at the end of World War II.

The Bay of Pigs provides a prominent example of how confidentiality can be misused to hide ill thought out schemes from closer scrutiny. It involved the attempted overthrow of Fidel Castro by a clandestine invasion force of 1,500 men, and numerous ships, with repeated air strikes. Despite the magnitude of the operation, American involvement was supposed to be plausibly deniable. However, rather than examine the operation's shortcomings in planning and implementation, this section will briefly discuss how the information pertaining to the invasion was handled, and how assumptions were tested.

The new administration was enthusiastic about this opportunity to demonstrate its ability to take charge and demonstrate its ability to stand up to Kruschev by standing up to Castro. Thus, a healthy skeptism was lacking amongst the Kennedy brothers. Matters were further worsened by their naiveté as to the ways of Washington. Professor Neustadt, for example, in a conversation with this student, said he believed that they were unaware

that this was an operation solely of the operational arm of the CIA. Believing that it had been approved by the intelligence arm of the organization, they proved all too willing to agree that in order to prevent leaks which could jeopardize the mission, both the State Department and the staff of the Joint Chiefs of Staff (JCS) should be prevented from knowing of the plan.

Since virtually everyone in the Miami Cuban community and a number of news correspondents were aware of the mission, such strenuous efforts at secrecy were at best wishful thinking. They did, however, have the advantage of shielding the plan from such unfriendly eyes as Roger Hilsman at the State Department. The further the plan progressed, the poorer its actual secrecy proved to be. Guatemala was awash in rumors. Senator Fulbright, Roger Hilsman, and Edward R. Murrow found out about it on their own.[1]

It seems highly unlikely that an operation which required the recruitment, in peacetime, of 1,500 people from a new and politically volatile community and the creation of a base in another small country could remain secret. Certainly the risk to its secrecy would not have been substantially increased by the plan being subjected to a searching scrutiny by three organizations who were at least as good at keeping secrets as the Cuban "freedom fighters;" unfortunately, the intelligence arm of the CIA, the State Department and the Bureau of Intelligence and Research, and the JCS were all excluded from evaluating the invasion.

The level of secrecy imposed, well above that used with respect to nuclear weapons,[2] only served to protect the plan from examination. The beneficiaries were, until the mission failed, the operation staff of the CIA. It seems reasonable to assume that at least part of Dulles's motivation was the desire to dazzle a new administration, and one in which the

President and his brother were infatuated with anything labeled covert or clandestine, with a new classic coup on a par with Iran and Guatemala.[3]

Such a success could only have strengthened the CIA's role in a "take charge" foreign policy. The Bay of Pigs, therefore, represents a classic case of the use of secrecy to gain personal and bureaucratic advantage, and to shelter a favorite but badly flawed scheme from scrutiny.

A less dramatic example of the use of secrecy for bureaucratic advantage was provided by Dr. R. V. Jones's* description of Michael Perrin and Eric Welch's successful effort to gain control, at the end of World War II, of intelligence with respect to German nuclear weapons development.[4] Dr. Jones (who had set up Perrin and Welch in this business) and his staff attempted to arrange for the captured documents or their photocopies to be delivered to his department for evaluation. According to Dr. Jones, at the last moment, the delivery to England of the documents for photocopying was cancelled by the Americans because Perrin and Welch claimed that his staff was not secure enough.[5] As the staff had been privy to virtually every important secret in the war including Ultra, the accusation seems to have been at best unfounded. However, as a result of this accusation, the documents were flown across the Atlantic to the U.S. without copies having been made. Had the aircraft crashed, by no means an unheard of event either then or now, all would have been lost.[6] Thus, the use of secrecy to ensure a bureaucratic position placed at considerable risk valuable information even as it ensured that "Perrin and Welch held the whip hand in all nuclear intelligence matters.[7]

---

*Head of Scientific Intelligence for Britain Air Staff and Scientific Advisor to M16 during World War II.

In Dr. Jones opinion this led to several unfortunate consequences. First, while he felt Perrin and Welch did their job of evaluating the results competently, it meant his staff was less well-informed than was desirable for their mission of overall evaluation of scientific intelligence. Second, this exercise in empire building led to the division of the scientific intelligence community into factions. As information is power, especially in intelligence, once one participant begins to hoard or is felt to be hoarding information for organizational and/or personal advantage, the others also begin to hoard in self-defense. This can and did, according to Dr. Jones, rapidly transform a process characterized by close interdepartmental cooperation into one in which the principal enemy was one's colleagues.

The restriction of information on the real problem from "the competition" must inevitably reduce the efficiency of the overall process, thus wasting manpower, resources, and information.

These two incidents highlight several of the key questions which should be asked by policy makers when confronted with a request to impose secrecy on an operation or an area of intelligence. Why is this request being made? Who will benefit from it? Is it to protect an important secret? Is the secret impossible to protect because it is already known, or the operation is too big to be hidden? What are the risks inherent in too narrowly restricting information? Will this veil of secrecy prevent the appropriate evaluation of a project, will it restrict information from those who can shed light on it, or will it protect sources and methods? Finally, will withholding information accomplish anything?

Because information is power, policy makers must guard against the misuse of secrecy by advocates and those with ambition. Failure to do so

can inhibit the testing of assumptions, analysis and conclusions, and it will also lead to organizational infighting. The battles which will inevitably erupt for control of this precious resource can only reduce the efficiency of the intelligence process.

Evaluation of Intelligence

The Bay of Pigs provides an important example of the possible consequences of the withholding of information from those able to comment intelligently upon it. Dr. Jones, in his book The Wizard War, explores in detail how the British managed the acquisition and evaluation of scientific intelligence. In his opinion, in order for there to be an efficient evaluation of such material, there had to be one central body of qualified experts which received all the information available to the government. This body would have the responsibility of evaluating the information and releasing it to the appropriate authorities when the time was right. He also warned against the danger of the premature release of information to policy makers before it had been fully evaluated.

> We are sometimes criticized for withholding information, but while no instance has ever been proven, we reserve our right to do so because (1) to spread half-truths is often to precipitate erroneous action by the Air Staff, and (2) the steady and immediate broadcasting of such significant, and unsolicited fact automatically and insiduously acclimatizes the recipient to knowledge of enemy developments, so that they feel no stimulation to action. The presentation of the complete picture of an enemy development is the best way of stimulating the appropriate authorities to action. The production of such pictures involves much effort, but it has been justified by results. Although we think the above policy is the best, it obviously has some defects which we try to remedy by frequent oral communications to the appropriate bodies.[8]

Complete intelligence regarding the German V-2 was sent to several locations. This was to have several results--some perverse. First, "a

very able intelligence officer" (in the War Office) "there came to the same conclusion"[9] that the Germans were developing a military rocket; and, at almost the same time, Dr. Jones felt that his duty was to notify Churchill's Science Advisor (Lindemann) and to pursue this possible development as energetically as possible.[10] The officer in military intelligence, however, chose a different course of action. "He warned the Director of Military Intelligence, who in turn warned the Vice Chief of the Imperial General Staff, who became so concerned that he took the matter to the Vice Chiefs of the Imperial General Staff."[11] They in turn were so concerned that "General Ismay, Chief of Staff to the Minister of Defense, minuted the Prime Minister."[12] The Chiefs' recommended that a "single investigator be appointed to call on such Scientific and Intelligence Advisors as appropriate, and suggested the name of Mr. Duncan Sandys."[13]

This, according to Dr. Jones, was to lead to the formation of a committee, and once the bombs started falling, to an explosion of such committees. The committees' membership, while highly distinguished in most cases according to Dr. Jones, was singularly unqualified to deal with the V-2's performance, capabilities, and rate of deployment. The committee overestimated the V-2's weight, payload, failed to recognize that it could be liquid fueled,* and believed that an inappropriate method of construction would be employed.[14]

Dr. Jones, despite his obvious disappointment at the creation of a committee to make evaluations which he felt were being competently done by his staff, claimed to have behaved in a responsible fashion. He saw to it that

---

*Liquid fuels at the time allowed for much greater thrust than did solid fuels.

"besides passing on to Sandys (head of the committee) any information we might obtain, and making efforts to get it by means that might not occur to him and his advisors, I would continue to collate all information as a reserve if he and his organization ran into difficulties."[15]

While Dr. Jones argues persuasively that many more people were brought into the evaluation process than was necessary and that much effort was as a result wasted, several other points are worth considering.

First, the information came from a variety of sources, agents, photo reconnaissance, radio intercepts, and cryptography. Both the compromise of the agents and the cryptographics would have been a serious blow. Nevertheless, the information and evaluation were circulated to all who might in theory have been able to benefit from it. This meant that both Dr. Jones and military intelligence were able to spot the threat in a timely fashion and to achieve a consensus as to its seriousness. Second, while Dr. Jones was amused and horrified by the committees' incorrect conclusions, it is important to note that ultimately the real threat was identified. Third, by having to justify his staff's conclusions in the face of competing theories, he and his staff were probably spurred on to greater efforts in information gathering, evaluation, and in creating a convincing case to present to the policy makers.

The V-2 story also demonstrates the importance of multiple sources of information, the fruits of which, even if only in a sanitized version to protect sources, are allowed to circulate freely amongst those who might be able to shed light on a subject. A telling example was the role of photo reconnaissance in this saga. Dr. Jones, but not the photo interpreters, was able to spot the V-2 at its new test site in Blinza, Poland and also to recognize that it was so well gyro-stabilized that it

could have been launched from a simple concrete platform, explaining why no obvious launching sites had been seen in range of Great Britain.

Likewise, the deciphering of the German codes provided much useful information on the performance of both the V-1 and V-2.

Finally, the V-2 demonstrates the risks of relying solely on one set of experts. If Dr. Jones is to be believed, his staff was always right and the various committees were invariably wrong. However, had he been excluded from the entire process, the intelligence officer in the War Ministry would still have sounded the alarm. Had the government then depended solely on the panel of experts it assembled, the right answers might have been delayed or never reached.

The key issue raised by the V-2 story for the evaluation of intelligence is what is the maximum number of people able to contribute constructively to the process without jeopardizing sources and methods.

A number of key pieces of information were located because of specific requests of the analysts (for example, requests for photo reconnaissance). This demonstrates the importance of the analysts being able to communicate their needs to the gatherers. Thus the interchange between analysts and the communication of their needs to the gatherers is an important part of the intelligence process.

The increasing complexity of the world in the 1980's means that effective analysis will require the utilization of talent in academia and the private sector. This, coupled with the more active role Congress has played in recent years in foreign policy, has created new requirements for the broad-based distribution of information acquired from sensitive sources.

Appropriate means of sanitizing the material to protect sources and

methods will have to be developed. The problems and issues of control involved correspond closely to the problems of the operational use of intelligence. The next section, therefore, will deal with how sensitive information can be distributed and when it should be withheld.

THE OPERATIONAL USE OF INTELLIGENCE

Because of the wealth of published material pertaining to the role of cryptography during World War II, most of the examples examined here will be related to the decision to use or withhold such information from field commanders.

The examples chosen are the British use of naval-related intercepts to sink Rommel's supplies in the Mediterranean, the bombing of Coventry, the American use of their cryptographic breakthroughs in the Pacific, and finally, the decision to take no obvious precautions to deal with the German attack scheduled for December 16, 1944 in the Ardennes.[16] Cryptography was essential to the prosecution of World War II by the Allies in both the Atlantic and Pacific theatres.

The most famous incidents in the Pacific theatre in which cryptography was essential to success were the Battle of Midway and the shooting down of Admiral Yamamoto. In both cases the stakes involved were clearly great enough to justify the risk of losing the source.

The loss of Midway could have enabled the Japanese Navy to dominate the Central Pacific, thereby increasing the difficulties the U.S. would have faced. Thus while the Japanese had intended to decoy the U.S. carriers to the Aleutians with a feint to Dutch Harbor,[17] the very importance of the island meant that there was nothing which pointed directly toward cryptography as the reason for the U.S. carriers being on station.

Admiral Nimitz briefed his commanders as to the expected Japanese actions, but never mentioned to them the source.[18] This caused Rear Admiral Theobald (Commander of the Naval Forces of the Aleutians) to disbelieve the

intelligence supplied him and to deploy his forces inappropriately.[19] With respect to the actual battle, standard naval reconnaissance activity by shore-based aircraft succeeded in locating the Japanese carrier forces, but not the surface fleet with Admiral Yamamoto aboard--which was only a few hundred miles behind the carriers.[20] Nor had cryptoanalysis indicated the combined fleets' role in the attack on Midway. Admiral Spruance, therefore, deserves full credit for his decision not to risk a surface engagement after the major carrier exchanges of June 4.[21]

Admiral Nimitz demonstrated in this battle that it was possible to disseminate information widely as a general intelligence summary without jeopardizing the sources. Getting the commanders to actually use the information is another problem beyond the scope of this paper.

One of the key questions in the operational use of intelligence is: can sensitive sources be protected by including the key information in a sanitized form? As Mr. William Colby has pointed out in his classroom presentation, this is possible more often than is generally believed.[22]

The decision to intercept Admiral Yamamoto's plane was at best a difficult one. If Yamamoto was shot down, would he be replaced by a better officer?[23] Commander Layton, chief of naval intelligence accurately surmised that any replacement could only be inferior in comparison.[24] He also pointed out that Yamamoto's death would be a tremendous blow to Japanese morale. Nimitz, therefore, concluded that a successful interception would be the equivalent of a major victory.[25] Interception would require land-based aircraft operations at maximum range. It was highly likely that the Japanese would conclude that their codes had been broken. However, no major allied operations were planned for the next two and one-half months.[26] The Japanese

had already several times changed their codes including a much delayed change just before the Battle of Midway. Each time the codes had been broken. Given the limited resources now available to the Japanese, it was highly unlikely that a new commander would be able to mount any serious operations before the expected cryptographic breakthrough. Admiral Nimitz, therefore, concluded that the risk return relationship was favorable and authorized the operation. To minimize the chances that the Japanese would determine cryptography was their weakness, Admiral Nimitz ordered the acting area commander (Vice Admiral Wilkinson) to brief all personnel involved with a cover story. This story claimed that the information was based on reports from the much respected Australian Coastwatchers who had in turn received it from friendly natives on Rabaul.[27] To further minimize Japanese curiosity, Admiral Nimitz ordered that the Navy give no publicity of any kind to this operation.[28] Fortunately, while Washington was soon buzzing with at least the outline of a correct story, the Japanese did not become aware.

In the Mediterranean, the war in North Africa was a see-saw with both sides' operations assisted by the deciphering of each other's codes. Because of the British cryptographic skills, the allies concentrated upon severing Rommel's supply lines during his retreat to Tunis. Rommel's headquarters received a message notifying him when each supply convoy sailed, its course and destination.[29] The British, to protect their source attempted to arrange for each convoy to be spotted by a reconnaissance aircraft before it was attacked.[30] Unfortunately, one convoy remained hidden in fog after it sailed. It was critical that Rommel not be resupplied. Thus, despite the lack of an appropriate alternate explanation, the convoy was sunk.[31] This aroused the German curiosity and the Abwehr began an investigation

which proved unable to account for the leakage.[32] To help throw the Germans off the scent, a congratulatory message was sent to a non-existent agent in Naples, in a code the Germans were known to be able to read, congratulating him and raising his pay.[33] This eventually led to the Italian admiral in charge of the port being relieved of his post on suspicion of being the source.[34]

Less easy to deal with is the decision to withhold information from those who can benefit operationally from its transmittal. A classic case was provided by the German bombing of Coventry. The British were with considerable success, reading the Luftwaffe Enigma encrypted signals. The information was used, in conjunction with radar, by Air Marshall Dowling to inflict maximum damage on the Luftwaffe with minimal force. Because the source of this information was so tightly held, his group commanders, especially Leigh Mallory, were so incensed at what to them was the wrong strategy that they forced through a high level meeting in October to criticize Dowling.[35] This afterward led to his replacement. An interesting example of being fired for doing everything right.

On November 14th at about 3:00 p.m., the British received the usual notification of an impending German raid. In addition they were able to determine that Coventry was the target.[36] (The official history maintains that the Air Ministry had two days' notice of the raid.)[37] Coventry was a heavily populated industrial city. Evacuation of the population might have saved lives, if the logistics could have been handled, which is by no means clear. The Germans, despite the British success at rounding up their spies and using them as double agents, would almost certainly have noticed the city's evacuation. Given the Royal Air Force's (RAF) precarious position and the

importance of the Ultra cryptographic success to the managing of the Battle of Britain, Churchill, who modestly does not discuss the issue in his memoirs, decided to have decoy fires lit and to notify the emergency services in the affected area.[38] Because of the British counter-intelligence successes, this low level response had a relatively small chance of jeopardizing Ultra. The decision, while almost certainly correct, could not have been easy. The key factor appears to have been the sheer indispensability of source, and the high probability of its detection if it were used in a manner that could not be readily attributed to radar or Dowlings' eccentricity.

The final incident to be examined is the Battle of the Bulge. I was able to locate where microfilm copies of the relevant documents are kept. Unfortunately, the nearest depository was in Washington.* It, therefore, proved impossible to confirm with documents Dr. Hickman's (who at the time ran SHAEF's top secret filing system) oral history. However, because of the quality of his scholarship I am willing to accept his story subject to later confirmation.

The thesis is that SHAEF not only received the appropriate indications of the impending German attack,[39] but correctly evaluated and used them. It is alleged that SHAEF wanted the Germans to have a successful initial attack. It was then intended to counter-attack, destroying the cream of the German forces on the Western Front, thereby shortening the war, reducing Allied casualties, and ensuring a more favorable position for the post-war

---

*Complete records of SHAEF are kept in both Washington and London under record group 331, Records of Supreme Headquarters Allied Expeditionary Forces, 120 rolls of microfilm, Guide to the National Archives of the U.S., G.P.O. 1974, p. 992.

world.

The night before the German attack was expected, a recently arrived and extremely green[40] division was due to be rotated up to the line. It was decided that to hold back the scheduled rotation might indicate to the Germans that either their attack was anticipated or that the stiff resistance a seasoned division could provide meant that achieving a breakthrough would be too costly. The rotation schedule, therefore, was followed and no one below the Army commander level was apparently informed. As expected, this division dissolved when attacked. What was not anticipated was that more seasoned troops would also panic, enabling the German thrust to penetrate much more deeply and inflicting much more damage than expected. It was eventually contained and forced back with heavy losses. The German casualties and the misallocation of their scarce military resources probably substantially reduced the cost of Montgomery's breaching of the Siegfried Line.

CONCLUSIONS

As one surveys the cases, certain key issues are illuminated. First, only occasionally was it necessary to withhold information at the operational level to protect the source. In most cases it was possible either to give a misleading indicator as to its origin or to sanitize the information in such a way as to avoid the source's disclosure. At the strategic level there seems even less excuse to withhold information as opposed to the source from those who can assist in its evaluation. Policy makers must guard against attempts by empire builders to restrict information for personnel or organizational reasons.

The key issue for the distribution of information, therefore, is not how tightly it can be held but how widely it can be distributed without jeopardizing the source. It was repeatedly demonstrated during World War II that it was possible through the careful sanitization of information from cryptography to widely distribute the evaluations and conclusions without jeopardizing the sources. Where the source was at risk, it was almost always possible to provide a false lead. In many cases there were a plethora of possible sources, which were used to sharpen the picture and to guard against false signals. Thus by acknowledging loudly those sources which were beyond the enemy's reach (for example, radar during the Battle of Britain), it was possible to avoid attracting attention to "the Ultra Secret." Likewise the Japanese attack on Midway was so obvious that there was little reason for the Japanese to suspect inside information. Indeed, as the last American torpedo bomber crashed into the sea, it appeared as though the Japanese objective--the destruction of American power--was about to be attained. The success of the remainder of the poorly coordinated attack by the carrier-

based dive bombers could only be blamed by the Japanese on bad fortune.

The decision to withhold information from those who can benefit from it operationally is a difficult one. First it runs the risk of setting off an organizational battle for control of such a critical resource. Second, it can only be done infrequently and where the gains are clear and evident. One does not undertake risky missions whether it be the introduction of a new product line or sailing in a convoy through hostile waters with the intention of being a "sacrificial lamb."

The knowledge that one was being treated in such a cavalier fashion can only have a deleterious effect upon morale and performance. Thus a decision such as the ones leading up to the Battle of the Bulge must be tightly held, and should not occur so often as to create a pattern which is discernible to either the opposition or the victim. The withholding of the sources of information by making the origin of intelligence materials uncertain and mysterious has an additional advantage of making it easy to claim that one never knew disaster was about to strike. Such behavior, at best, borders on immorality even in an amoral world. Therefore, only substantial need or expected gain can justify it.

POLICY RECOMMENDATION

The increasing complexity of the world and the requirements of Congressional oversight require a much greater degree of dispersal of potentially sensitive information than has historically been the case.

As was repeatedly demonstrated during World War II, it was possible to disseminate information widely without jeopardizing the source. The method most commonly used under Ultra and the American deciphering of the Japanese codes was to hold the source closely but to assure the commanders of the reliability of the material. The period also demonstrates how difficult it is for one's opponents to determine the source of one's information, even when they were intercepting and decoding messages which enjoyed a disturbingly high degree of accuracy. For example, for a substantial period of time, the Germans were able to read the British Naval codes. Nevertheless, as early as September of 1941 the Germans concluded that the British knowledge of the probable positions of the German U-Boats could have only come from reported sightings and radio reports.[41] The possibility that the German ciphers were being decoded was dismissed out of hand.[42]

The British, and where possible the Americans, always attempted to provide a misleading indication of where their information came from if its utilization operationally might have pointed to the source.

They also both attempted to ensure that information was available in a timely format to the end user. Conclusions with an indication of the reliability of the source have proved to be a time-honored means of disseminating information while protecting its origin.

One can therefore safely surmise that it is possible to disguise the source of information, thereby enabling its wider dissemination, without materially jeopardizing its utility.

To ensure greater confidence in the sanitized information, greater contact between the laundry operation, the gatherers, the analysts, and the users is desirable. As was pointed out in the V-2 incident, because Dr. Jones's scientific intelligence staff was in close contact with the sources of information, it was possible to request material which could shed light on a specific issue. These contacts helped reassure both the gatherers and evaluators that their opposite numbers seriously understood their needs and helped avoid the risk of sensitive information becoming a political football. A senior official in the National Security Agency has said to the author that with proper staff it would be possible to sanitize his agency's output in such a fashion that most of the material could be widely disseminated. Both he and Mr. Colby have stated that this could be readily done with most of the analyses produced by the intelligence community. Such a procedure, by enabling a much wider dissemination of hitherto sensitive material, would help mitigate the current practice of leaking sensitive and unsanitized material in the bureaucratic wars of the government.

The cost of such a sanitizing mechanism for the entire intelligence community has been estimated by a senior official at between 200 and 400 million dollars per year. He did not feel that this would be a significant increase in the intelligence community's budget.

In summary, for information to be evaluated and utilized effectively the key question remains not how tightly can the information be held. Rather, what steps are necessary to enable the widest possible circulation of intelligence based on sensitive sources and methods.

NOTES

1. See for example, Schlesinger, Arthur, Jr., A Thousand Days, Fawcett Premier Books, New York: 1965, pp. 235-242. Also see Kirkpatrick, Lyman B., "Paramilitary Case Study: The Bay of Pigs," Naval War College Review, November/December, 1972, p. 40.

2. Kirkpatrick, "Paramilitary Case Study," p. 41.

3. Dulles is reported to have told the President that it had at least as good a chance as the Guatemala coup, Ibid.

4. Jones, R. V., The Wizard War, Coward McCann & Geohegan, Inc., New York: 1978, p. 309.

5. Ibid., p. 480.

6. Ibid.

7. Ibid.

8. Ibid., p. 334.

9. Ibid.

10. Ibid.

11. Ibid.

12. Ibid., pp. 334-335.

13. Ibid., p. 335.

14. Ibid., Chapter 38, pp. 332-348; Chapter 45, pp. 440-461.

15. Ibid., p. 335.

16. This incident was related to me by Dr. Warren L. Hickman, V. P. Academic Affairs and Professor of International Relations, Eisenhower College. From 1943 through June 1945 he was in charge of a top secret filing system at SHAEF.

17. Holmes, W. J., Double Edged Secrets, U.S. Naval Institute Press, Annapolis, 1979, p. 97.

18. Kahn, David, The Code Breakers, The Macmillan Company, New York: 1967, p. 571.

19. Ibid.

20. Op. cit., p. 96.

21. Ibid., pp. 97-98.

22. Transcript classroom session 8, p. 21.

23. Kahn, Codebreakers, p. 598.

24. Ibid.

25. Ibid., p. 599.

26. Ibid.

27. Ibid.

28. Ibid., p. 601.

29. Winterbotham, F. W., The Ultra Secret, Harper & Row, New York: 1974, p. 79.

30. Ibid., p. 80.

31. Ibid.

32. Ibid.

33. Ibid.

34. Ibid.

35. Ibid.

36. Ibid., p. 60.

37. Ibid., p. 61.

38. Ibid.

39. According to Winterbotham, at least one of SHAEF's Intelligence Officers, Monk Dickson in Estimate No. 37, on December 10th, stated that the German buildup indicated an offensive. Ibid., p. 179.

40. The troops were so green that they needed their flashlights to find their foxholes.

41. Lewin, Ronald, Ultra Goes to War, McGraw-Hill, New York: 1978, p. 212.

42. Ibid.

SELECTED BIBLIOGRAPHY

Colby, William & Forbath, Peter, Honorable Men, Simon & Shuster, New York: 1978.

Halperin, Morton, et. al., The Lawless State, Penguin Books, New York: 1977.

Holmes, W. J., Double Edged Secrets, Naval Institute Press, Annapolis: 1979.

Jones, R. V., The Wizard War, Coward, McCann & Geoghegan, Inc., New York: 1978.

Kahn, David, The Codebreakers, The Macmillan Co., New York: 1968.

Kirkpatrick, Lyman B., "Paramilitary Case Studies: The Bay of Pigs," Naval War College Review, November/December 1972, pp. 32-42.

Lewin, Ronald, Ultra Goes to War, McGraw Hill Book Co., New York: 1978.

Schlesinger, Arthur, Jr., A Thousand Days, Fawcett Premier Books, New York: 1965.

Winterbotham, F. W., The Ultra Secret, Harper & Row, New York: 1974.

4. RE-SHAPING AMERICAN MILITARY INTELLIGENCE: DECISIONS FOR THE 1980's

Kenneth Allard

TABLE OF CONTENTS

LIST OF FIGURES

INTRODUCTION

The American military intelligence establishment has entered the decade of the 1980's after having experienced many of the same traumatic effects of post-Vietnam and post-Watergate re-appraisals that have also dominated the attention of the larger national intelligence community. Together with the increasingly public questioning of intelligence priorities and the legitimacy of the "sources and methods" used in carrying out operational missions worldwide, there has been the realization that in intelligence matters, as in so many areas relating to national security, there is simply no substitute for clarity in determining management objectives or in setting up precise, accountable lines of command and control to achieve those objectives. For the Defense Department, this has meant a new commitment to the idea that the intelligence assets under its immediate control should have as their primary mission the production of intelligence which directly contributes to the objective of fighting and winning the nation's wars.

Of the intelligence agencies within the Defense Department, none have been more profoundly influenced by this increased focus than the Military Intelligence (MI) Branch of the United States Army. Although formally constituted as a branch of the regular Army only since 1967, MI has seen basic changes in its organizational imperatives during those 13 years, changing from an entity which was primarily a strategic asset with some limited tactical functions to one in which just the reverse now seems to hold true. To better accomplish tactical intelligence objectives, for example, a major initiative is presently being taken by the Army which will place dedicated intelligence collection and electronic warfare assets within the organizational structure of each combat division; similar plans call for the formation

of comparable units at corps and even theater army levels. Even while these tentative plans are being worked out in the nether worlds of position papers, coordination drafts and policy statements, even more far-reaching de facto revisions have already been made in the policies of the training bases and the personnel directorates -- all of which reflect the fact that "tactical is the way to go" for the upwardly mobile young MI officer or enlisted man.

It thus seems appropriate, in the light of these incipient changes, to review the process as it has developed to date in order to identify the management decisions which are necessary in order to insure that the initiatives which have been taken thus far can be linked successfully to the larger questions of command and control at the strategic level -- for which military intelligence also provides a critical input. Indeed, the idea that the military intelligence structure is -- or should be -- an organic one, encompassing military echelons from maneuver battalions to the Joint Chiefs of Staff, suggests three basic questions:

1) How should military intelligence be structured in order to provide support to commanders at both tactical and strategic echelons?
2) In what ways must the military intelligence structure be shaped in order to insure that its inputs at the strategic level complement those of other service intelligence agencies (Navy and Air Force), as well as those of national-level intelligence organizations, such as the CIA?
3) How should the military intelligence system be structured in order to insure that it functions adequately in wartime (conventional, limited nuclear and general nuclear wars) as well as more limited crisis management and that its products are available to military commanders and national decision makers under all of these conditions?

This paper represents an effort to examine these questions and to highlight management alternatives available to achieve what must be seen as the final objective of this organizational approach: the creation of a balanced "architecture" for MI which, despite its importance at the tactical level, remains an asset of strategic importance as well. In order to understand the milieu in which these issues are being hammered out, however, it is first necessary to describe the changes in military science which have provided the evolutionary pressure for corresponding adjustments in the methodology of military intelligence at all levels. That understanding is basic to the section which follows and describes the shape of the tactical intelligence structure now being put together. Several recent publications have also made it possible to discern the shape of the Army's thinking on the future of the strategic intelligence system, primarily for the "echelons above corps," i.e., at Army and theater Army levels, including the critical link to national command levels; that structure as it now appears is the subject of the section, Military Intelligence at the Strategic Level: Old Imperatives, New Realities. While the parameters of potential management issues are addressed as they arise in the course of the discussion, the final section of the paper presents an analysis of their implications.

BACKGROUND

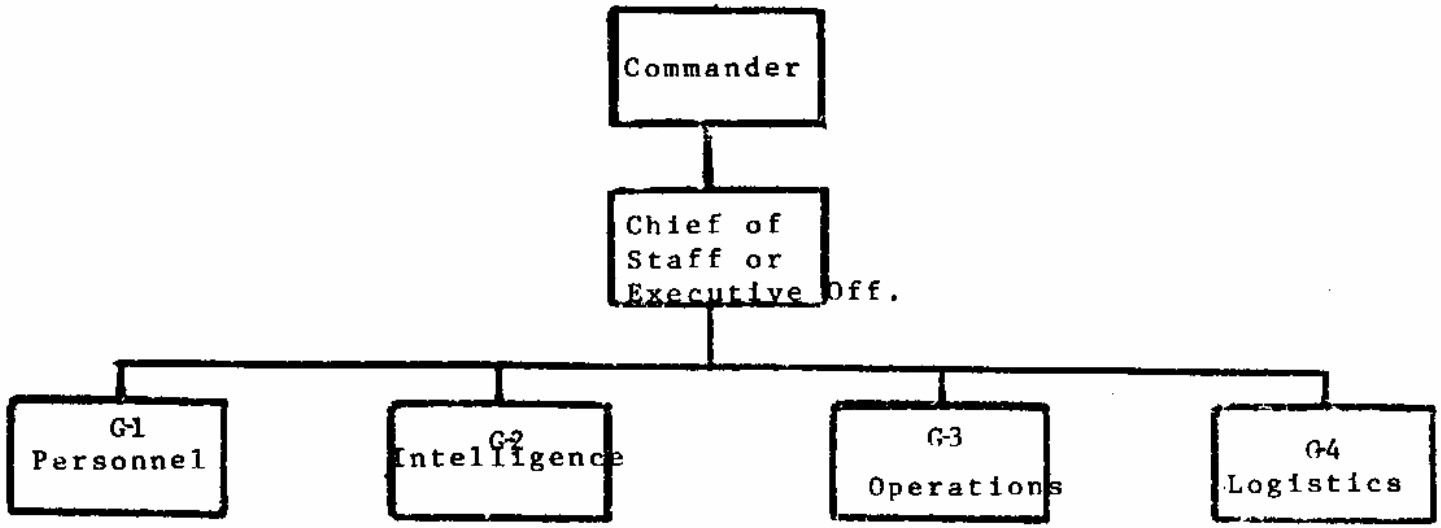
It would be unfair to suggest that the U.S. Army has traditionally ignored the importance of intelligence in its tactical operations; it is a fact, however, that there were no formal provisions for intelligence representation on tactical command staffs until World War I, when General Pershing reorganized the staff structure of the Allied Expeditionary Force to conform

largely to the British model. This division of the staff into separate components for administration, intelligence, operations, and logistics (called G-1, G-2, G-3, and G-4, respectively) represented a change which has largely survived to this day, as shown in the chart at Figure I. It did not, however, guarantee that there would be an effective integration of operations and intelligence during either training or war. For one thing, the G-3 as the operations officer tended to dominate the rest of the staff; not surprisingly, the G-3 office also tended to attract the most capable and ambitious officers, who were themselves regarded as the heart and soul of the command staff and earmarked for greater things. The G-2 staff did not enjoy the same regard, and this tendency eventually caused problems when next the American Army found itself at war. Omar Bradley's memoirs contained a passage which is still relevant:

> The American Army's long neglect of intelligence training was soon reflected by the ineptness of our initial undertakings... In some stations, the G-2 became the dumping ground for officers ill-suited for command. I recall how scrupulously I avoided the branding that came with an intelligence assignment in my own career. Had it not been for the uniquely qualified reservists who so capably filled so many of our intelligence jobs throughout the war, the Army would have been pressed....[1]

Despite Bradley's tenure as the post-war Chief of Staff and the striking success of Allied intelligence operations during the latter phases of World War II, Army Intelligence continued to be looked upon in many of the same ways as before.[2] Even though the wartime Counter-Intelligence Corps became the post-war Intelligence Command, and the elite staff of Army cryptologists was reorganized into the more formalized structure of the Army Security Agency (ASA) in 1945, Army officers were still not systematically trained in intelligence matters at the tactical level. The feeling seems to have been

FIGURE I: STANDARD ARMY STAFF ORGANIZATION AND FUNCTIONS



MAJOR FUNCTIONS:	G-1 Personnel	G-2 Intelligence	G-3 Operations	G-4 Logistics
	Administration	Intelligence	Ops. planning	Supplies
	Records	Security management	Training	Maintenance
	Personal actions	Physical security	Operational Scy.	Budgeting
	Law enforcement	Maps	Electronic warfare	Services

NOTES: A. The general rule of staff procedures is--the higher the staff, the more elaborate it becomes. The level illustrated here shows the most common breakdown of staff responsibilities among Army units. At battalion and brigade levels, the G-staff arrangement is the same, but it is referred to as an S-staff: S-1, S-2, etc.

B. The G-3 functions for Operations security and electronic warfare are traditional, and, as such, are the subjects of much debate in the formation of the CEWI concepts.

that counter-intelligence and signals intelligence were important as specialized functions of higher command, and that their peacetime functions required their continuance as strategic assets. However, words such as "specialized" and even "strategic" contrast rather sharply with the ethos of the professional officer whose career progression more often depends upon his being perceived as a generalist with a wealth of tactical experience. Bradley's critique continued to be valid, with only those officers being detailed to intelligence duties who could be spared elsewhere.

One also suspects that the Army leadership may have been influenced by at least one of the dimly remembered teachings of Clausewitz hammered into them as cadets:

> A great part of information obtained in War is contradictory, a still greater part is false, and by far the greatest part is of a doubtful character. What is required of an officer is a certain power of discrimination, which only knowledge of men and things and good judgment can give... In a few words, most reports are false, and the timidity of men acts as a multiplier of lies and untruths... Firm in reliance on his own better convictions, the Chief must stand like a rock against which the sea breaks its fury in vain.[3]

The idea that a commander's powers of discrimination and good judgment are of greater value than "information" of dubious value strikes a responsive chord among many Army officers to this day, particularly those in the combat arms of infantry, armor and artillery. The example most frequently cited in this regard is not so much Clausewitz but Douglas MacArthur, who regularly overruled his staff and actually executed his most daring operation at Inchon against the best intelligence and operational advice his staff could offer.[4] This is not to suggest that the American officer corps affects a "know-nothing" attitude toward intelligence or that it has a predilection for ignoring facts. What is suggested is that there has been a traditional tendency

for commanders and staffs at the tactical echelons to place primary emphasis on combat "information" gathered as the result of operations conducted against the enemy and reported through the chain of command and not on the results of strategic intelligence gathered through mysterious means and beamed down to the battlefield from on high. It is well summed up in the old dictum, "The best way to get intelligence is to fight for it."

This philosophy proved to be inadequate for the problems encountered during the Vietnam War. Army commanders there from General Westmoreland on down found that, although their training had prepared them well for the efficient employment of overwhelming tactical force backed by elaborate fire support mechanisms, their chief problem now consisted of locating a highly elusive enemy. Even more vexing was the ability of the guerrilla to blend in with his surroundings, emerging to fight only when he enjoyed a decisive advantage. One general officer commented on these perplexities:

> ...I knew that finding the enemy would be one of our toughest jobs. It occurred to me that perhaps we would be able to identify the guerrilla, a farmer by day and a fighter by night, by the dark circles under his eyes. As it turned out, our surveillance was just about that sophisticated.[5]

The response to these difficulties was primarily technological, as were so many other features of the American experience in Vietnam. To the traditional fields of signals intelligence (SIGINT), counter-intelligence/human-intelligence (HUMINT), and imagery intelligence (IMINT), an entirely new array of sensors was added. Battlefield radars, new types of reconnaissance aircraft, unattended ground sensors and infrared photography all provided an increasingly technical base to the development of intelligence. Other air-

borne sensors sought out enemy radio signals and flashed the location of the sender back to artillery units on the ground. HUMINT teams sought out the enemy infrastructure through computer-assisted pattern analysis and, in some cases, directed infantry units to the targets thus developed. Almost overnight, military intelligence had become an important part of the battlefield target acquisition process and an increasingly visible part of operational planning. A milestone appeared to have been reached when, partly because of the increase in manpower caused by the war, Military Intelligence (MI) was formally constituted as a branch of the regular Army in 1967 and a permanent corps of officers assigned to it.

The lessons learned from the guerrilla war in Vietnam had not been fully absorbed when the 1973 Arab-Israeli War provided a highly influential object lesson in the impact of modern technology on more conventional battlefield outcomes. Adding to the significance of the observations made possible by the conflict was the fact that, more than in previous Middle East Wars, there was a direct face-off between protagonists wielding U.S. and Soviet top-of-the-line equipment. This was also the first such conflict in which electronic warfare had such demonstrable results on ground combat, as Soviet-supplied air defense radars operated with deadly effect against Israeli planes, limiting the ability of that arm to redress the traditional numerical superiority of Arab armies. Equally impressive were the results of a variety of munitions which, either through improved sighting or terminal guidance systems, were able to exact a much higher 'probability-of-hit' ratio than had ever been seen in comparble combat. Largely for that reason, there was an unprecedented attrition of forces on both sides that, for a time, appeared to prejudice the ability of the superpowers to effect timely re-supply of their

client states.[6]

The parallels with a war between the Warsaw Pact and NATO armies in Central Europe were obvious and, given the close-run nature of the Israeli victory, more than a little disturbing. The numerous debriefings, special studies and analyses which were done in the aftermath of the 1973 war resulted in a sweeping revision of the Army's tactical doctrine, and the publication of an important new field manual on operations, FM 100-5. This document, "the capstone of the Army's system of field manuals,"[7] was intended to write a new chapter in the way the Army went about the business of preparing for war, and to put commanders at all echelons on notice that a new era had begun:

> The war in the Middle East in 1973 might well portend the nature of modern battle. Arabs and Israelis were armed with the latest weapons, and the conflict approached a destructiveness once attributed only to nuclear arms.... In clashes of massed armor such as the world has not witnessed for 30 years, both sides sustained devastating losses, approaching 50 percent in less than two weeks of combat. These statistics are of serious import for U.S. Army commanders.[8]

The manual went on to analyze the changes which had occurred in land combat, beginning with the tank. Because of the improvements in armor, firepower, and maneuverability, "the capabilities of modern tanks have been extended to as far as the tanker can see. What he can see, he can hit. What he can hit, he can kill."[9] Interestingly, the manual also noted that precision-guided anti-tank missiles had significantly increased battlefield lethality by achieving 90 percent probabilities-of-hit at ranges out to 3000 meters.[10] These weapons were increasingly being proliferated among both mechanized and conventional infantry units, giving them for the first time the ability to engage armored targets at extended ranges. The manual discussed the additional mobility brought about by the increasing

mechanization of infantry forces, but failed to mention that the Soviet "motorized infantry" had the advantage of having an armored personnel carrier which carried as much firepower as most World War II tanks, while also incorporating impressive gains in cross-country mobility. The third traditional combat arm, artillery, also came in for some attention, the trend being that "revolutionary advances" in projective lethality now made point destruction of individual targets possible through the use of laser designators.[11] Indeed, Chapter 7 of the manual went into an unprecedented endorsement of the idea that intelligence is "the commander's responsibility and provides the basis for tactical decision."[13] Despite the long heritage of indifference to these matters, tactical commanders were now being told that they were responsible, through their G-2 officers, for the effective management of three intelligence disciplines:

1) electromagnetic intelligence -- including signal intelligence, cryptanalysis, communications analysis and traffic analysis, ground surveillance radars (GSR's) and remote sensors (REM's).
2) imagery intelligence -- "derived primarily from radar, infrared and photographic sensors carried by overhead platforms."
3) human intelligence -- including prisoner-of-war interrogation, reconnaissance patrols, front-line observation, and counter-intelligence operations.

Making all of these assets work together would allow commanders to "see"[14] their adversary on the battlefield, to pinpoint the location of his main forces and to take them under fire at long ranges, thereby reducing the number which would survive to attack American front-line units.

Still another dimension which commanders would have to consider was implied by the proliferation of the new battlefield sensors which were also known to be present in Soviet-equipped armies. Obviously, the defensive side of protecting an American army in the field now demanded a more imaginative approach which would take account of the challenge posed to command operations security (OPSEC) by the new enemy collection systems. For example, traditional communications security had stressed the importance of codes; however, improvements in electronic direction-finding equipment now meant that radio transmitters could be located with a precision which made them attractive targets for enemy firing batteries. Therefore, the greatest threat to friendly communications might not be the decryption of codes, but simple destruction of the sending stations.[15] Concern for OPSEC was not new -- it had traditionally been a G-3 function -- but it now acquired greater urgency, gradually coming to embrace the total intelligence "picture" which friendly units presented to the full range of collection assets known to be available to a Soviet or Soviet-sponsored adversary. The people assigned to deal with this problem were the counter-intelligence specialists assigned to corps and division G-2 offices; they had increasingly been deprived of their traditional investigative functions in the post-Watergate era, but now found themselves responsible for "portraying the total threat environment" to the command. This change in emphasis fostered an awareness of the need for a "multi-disciplined approach" toward OPSEC, drawing from inputs suggested by each of the three major intelligence fields: SIGINT, IMINT, and HUMINT.

Much the same dynamic had also come to dominate the thinking of other MI professionals who argued that breaking down the barriers which had traditionally divided the three basic fields -- and particularly SIGINT -- was the

only rational way to produce positive intelligence on the battlefield and elsewhere. Here again, the principle of comparing multiple sources of information had long been a basic tenet of the theory of intelligence, but it was seldom carried out effectively in operational settings, largely due to the barriers of security compartmentation and functionally separate reporting channels. The main implication of this argument was that only by creating an entirely new organizational pattern for MI units in the field could the objective of "all-source" intelligence analysis and reporting be met.

By 1975, therefore, powerful forces were converging which would force a series of changes in the way the Army would look to its new military intelligence organization. The presence of MI units in some proximity to tactical commands, but without the traditional lines of command support, seemed an anomaly, particularly with the entirely new dimension of a growing demand for tactical intelligence. The proliferation of combat surveillance assets imposed a management problem of no small complexity that, it seemed, could best be solved by a centralizing of functions within the general realm of the tactical intelligence office. Finally, there was the internal consensus within MI itself that the need for integration of intelligence demanded a structural solution. In short, there was a clear sense that it was high time that Military Intelligence "got back in uniform and joined the rest of the Army."

COMBAT, ELECTRONIC WARFARE & INTELLIGENCE: THE NEW IMPERATIVES

Organization and Concepts

The problem of where and how to fit MI into the tactical structure of the Army became the subject of a major study commissioned by the Chief of

Staff, General Creighton W. Abrams. The group which was formed was headed by Major General Ursano, and in 1975 it issued its final report known as the Intelligence Organization and Stationing Study (IOSS). The report was a virtual indictment of the intelligence system which prevailed at the time. Its most serious findings were that military intelligence units were not properly organized to support the tactical mission and, indeed, were in most cases beyond the control of tactical commanders because of their strategic missions and functions. Given the fact that MI units existed under functionally separate chains of command and reported to different national-level agencies, the study concluded that, "The integration of intelligence from all sources into a single product was largely a myth."[16] It also recommended that the separate commands for cryptology and counter-intelligence (the Army Security Agency and the Intelligence Command, respectively) be combined at the strategic level and that a new structure combining all-source intelligence functions be created at the tactical level.

The IOSS study led directly to the formation of a prototype unit at Fort Hood, Texas in 1976-1977, which combined the functions of combat intelligence and electronic warfare known as the CEWI Battalion (for Combat Electronic Warfare and Intelligence, pronounced "see-we").[17] With a total strength of some 700 personnel, it incorporated sections for ground surveillance (battlefield radars and ground sensors), electronic warfare, OPSEC, imagery intelligence and interrogation. At its heart, however, was the "all-source production section" which for the first time set up an organic entity entity charged with tactical intelligence integration and dissemination. Structurally, the CEWI Battalion was organized as shown in the chart at Figure II.

The results of the operational tests at Fort Hood were not without the

usual problems encountered in any such experimental unit. One of the battalion's former commanders wrote:

> While the test results and experience have dictated certain organizational modifications and changes, the concept of consolidating all intelligence assets under a single commander at division level is sound and represents the key to successful tactical intelligence operations on future battlefields.[18]

While such testimony can hardly claim to be totally unbiased, much the same theme was echoed and re-echoed in the provisional CEWI battalions that other Army divisions in the U.S. and Europe organized on their own initiative from existing resources. In a recent article reflecting the perspective of a CEWI battalion in support of an airborne division, another CEWI commander stated that the organization, despite its problems, was "totally superior to its predecessors;" primarily because it was well-tailored to support a tactical mission, it provided a focus for integrating intelligence and EW in battle training, and it effectively channeled intelligence to the maneuver commanders who needed it most. Best of all, "CEWI provides aggressive intelligence and electronic warfare. CEWI actively seeks out the enemy."[19]

The enthusiasm for the CEWI structure has reflected a desire to see its final configuration officially approved and fielded in the expectation that whatever flaws it may have will be resolved through subsequent modifications as well as the informal tailoring which takes place in response to specialized missions. Accordingly, the final Table of Organization and Equipment for the divisional CEWI battalion was sanctioned by the Department of the Army in December 1979. Even in advance of this approval, however, preparations were rapidly being made to prepare final plans for the formation of a CEWI Group at corps level. The chart shown in Figure III depicts the three corps-level battalions of the CEWI Group with their major functional responsibilities:

operations (including all-source analysis and production); tactical exploitation (essentially all ground-based tactical surveillance and EW systems, and aerial exploitation (all airborne collection system). While this proliferation of functions may seem somewhat confusing for the uninitiated, the concept is quite simple: one unit concentrates on the ground surveillance mission, one on the aerial surveillance mission, and the central unit decides what it all means.

While the CEWI Group concept is still being analyzed, there is little reason to suspect that its final format will differ significantly from that presented here. For planning purposes, however, it has already been granted de facto approval since a number of major intelligence collection and processing systems have been designed around likely CEWI outlines. The complexity of the technology involved in many of these systems requires long lead times from conception to fielding; therefore the use of the CEWI Group as both a tactical focus and as a potential link to the all-important strategic echelon has been an essential working definition. While again, the caveats normally associated with developing systems apply, the illustration provided by the chart at Figure IV gives an idea of how the data flow from the major electronic surveillance systems will be organized at CEWI battalion and group levels.

The information flow itself is probably one of the most critical elements of the CEWI concept, since it involves the organization and comparison of data in unprecedented quantities. Complicating the matter still further is the idea that tactical intelligence must be "real-time" intelligence in order to have any value. Consequently the outlines of the all-source analysis system at both CEWI battalion and group levels (i.e., division and corps) have

FIGURE II: ORGANIZATION AND FUNCTIONS -- CEWI BATTALION (DIVISIONAL)

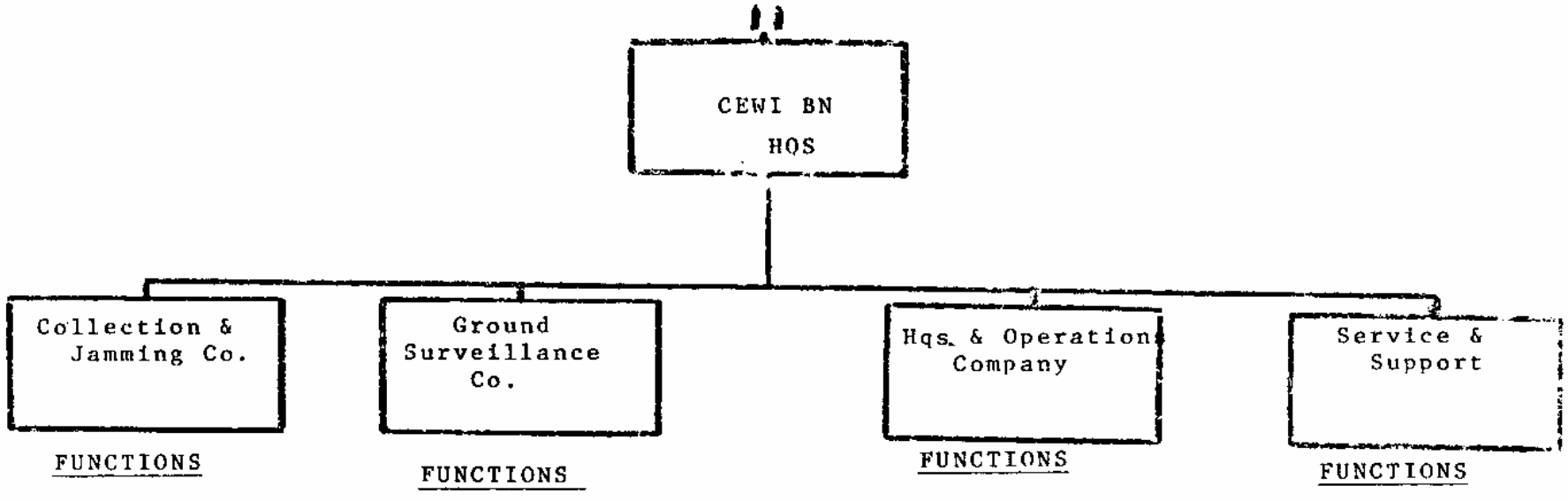
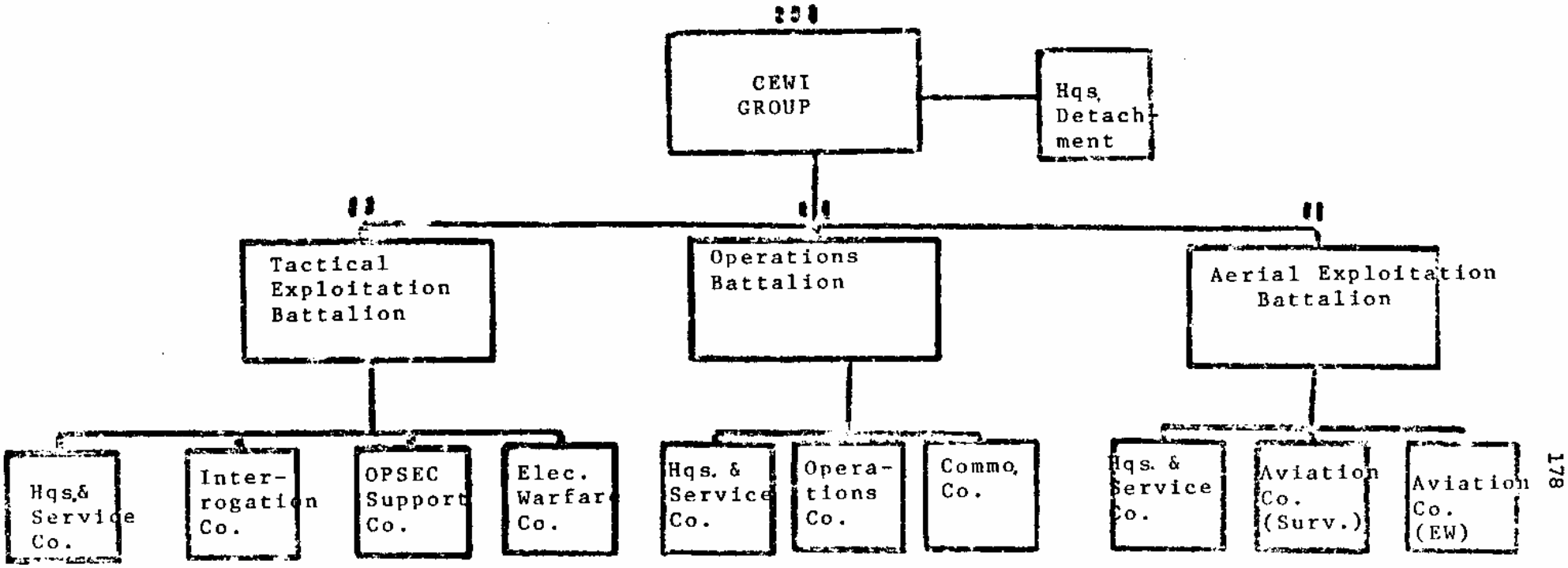


FIGURE III: CEWI GROUP (CORPS) -- ORGANIZATIONS AND FUNCTIONS



FUNCTIONS

Signals Intelligence
Electronic Counter-measures
Tactical Counter-intelligence
POW interrogation & document Exploitation

FUNCTIONS

Intelligence, electronic warfare, and OPSEC planning & management
Intelligence production & dissemination
Consolidated communications

FUNCTIONS

Airborne signals intelligence
Aerial photography

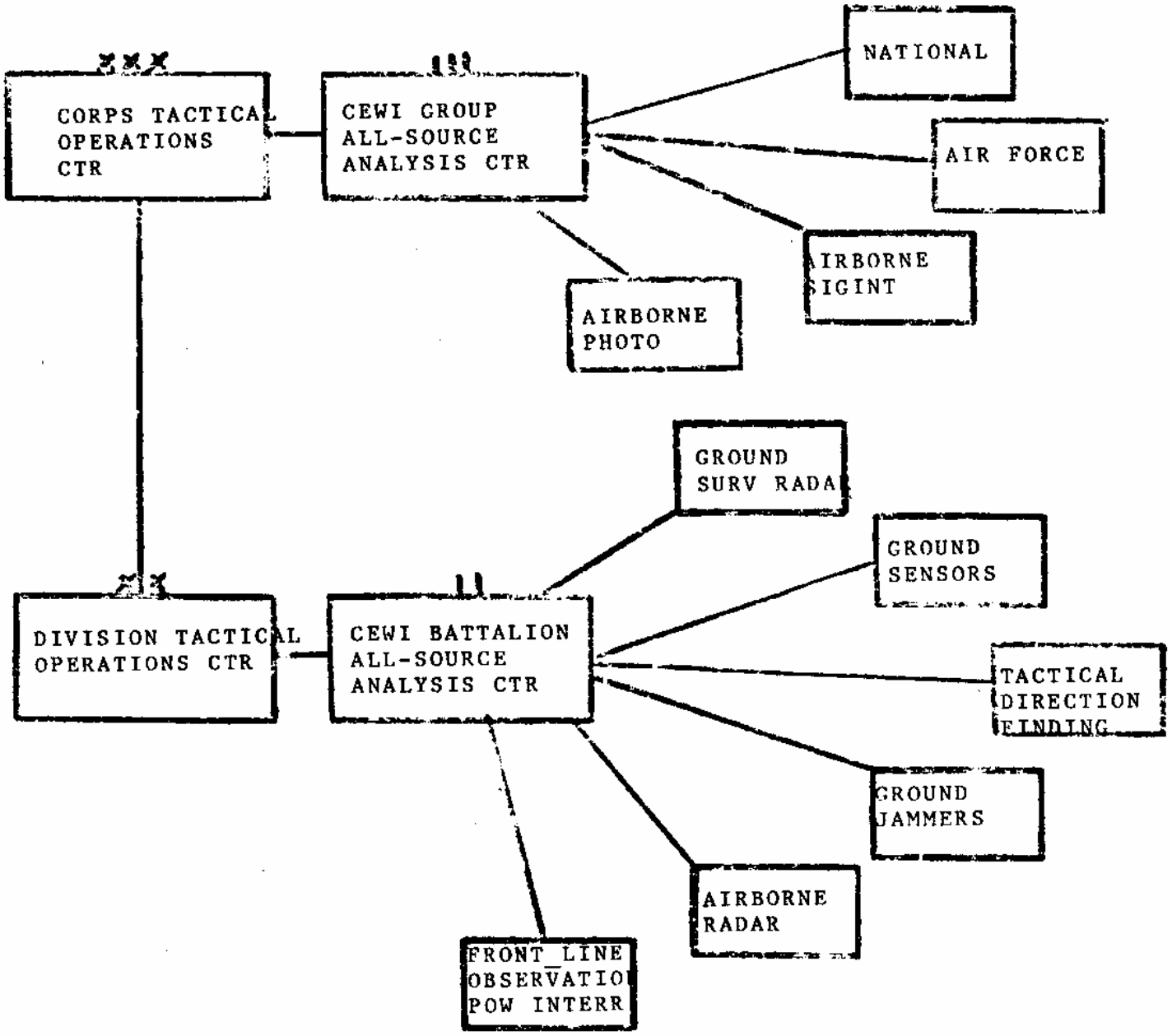
presupposed the use of automatic data processing equipment. A general officer who is probably the Army's most prominent spokesman on this topic -- Brigadier General Albert N. Stubblebine III -- made this point unequivocally clear in describing the highly complex task of "tracking" the 35,000 separate elements (i.e., the "movers, shooters and electronic emitters" comprising the most important fire and maneuver elements) in a typical enemy force targetted by the CEWI Group:

> Automation must be the savior, for only through a carefully designed automation architecture can one hope to search, sense, sort, sift, and select the right set of equipment or targets from the mass of 35,000. The human mind is a wonderful mechanism, but 35,000 is more than it can manage.[20]

In the same article, General Stubblebine went on to note that the move to automation further implied a need for miniaturized, compact ADP systems which could survive the environmental demands of a highly mobile battlefield. He also stated that the communications "mix" of sensor systems implied the necessity for "highly restricted message formats" in a major departure from previous practice.[21]

That suggestion raises an interesting point, since it would appear that the dimensions of a reporting system which seeks to collect data on some 35,000 targets through the use of multiple sensor systems would presuppose not just the use of an ADP system, but also the use of a common sensor language keyed to the capabilities of the computer software. The most likely approach to achieve such a system would be through the use of digitized communications plugged directly into the computer data base from the reporting sensors. In theory, the computer would periodically "interrogate" the sensors and would automatically correlate, focus and "fuse" the data for the intelligence analyst sitting in the all-source analysis

FIGURE IV: CEWI ORGANIZATION DATA FLOW AND REPORTING CHANNELS



center. From that point on, human judgment in its more traditional form would be used to flesh out the resulting picture of the battlefield. This concept -- or something very much like it -- represents the fundamental operating parameter of the CEWI system. Its other innovations -- centralized control of surveillance resources and the incorporation of electronic warfare assets -- also represent important changes with numerous implications not only for tactical intelligence, but for strategic intelligence as well.

Management Issues

From the discussion thus far, it is clear that there is a perceived need for a new tactical intelligence structure in the United States Army. The tentative structure advanced thus far under the CEWI concept offers a set of alternatives which provides a useful point of departure to assess the major questions which need to be clarified to insure that first, the tactical imperatives are met and that, second, they are met in such a way as to insure their congruence with the overall or strategic objectives of the intelligence system. This approach means that, rather than rejecting the CEWI structure out of hand or accepting it as a given, the analysis should focus on the major questions which this experiment has raised to date in order to determine the implications of future choices. These questions generally fall into four areas: operational/technical, methodology/ideology, communications, and resources. To a greater or lesser degree, of course, all of these questions are linked, particularly in the all-important area of resources, but for purposes of clarity they are addressed here individually.

Operational/technical.

1) The use of ADP systems not only creates a significant question in terms of resource allocation, but it also confronts planners with a non-trivial degree of inherent risk. Designing and building interactive sensors of all kinds with compatible micro-processing apparatus presents an array of technical questions which may challenge the state-of-the-art for some years to come. Complicating the problem still further is the question of battlefield survivability of such systems, not only in terms of mobility and durability, but also in terms of their vulnerability to the effects of electromagnetic pulse (EMP) from nuclear detonations. This vulnerability is particularly pronounced in those types of computer systems which would meet operational needs because of their use of microcircuitry and miniaturized memory banks. While some observers note that the use of such computers is made inevitable by the "pace of battlefield technology," others have suggested that the increasingly likely use of tactical nuclear weapons in even a "mid-intensity" U.S. - Soviet confrontation means that reliance on computer-assisted programs should not be absolute.

MANAGEMENT QUESTION: Do we accept this degree of technological and tactical risk, or do we hedge our bets by investing in other methods as back-ups?

2) The use of data bases is essential in any intelligence discipline. These bases are difficult, if not impossible, to maintain without significant inputs from strategic levels, particularly in the field of SIGINT. Equally important, data collected by the tactical systems must be made available to the strategic-level data base in order for it to remain

current. This is just one area, among a number of others, where the somewhat artificial distinction between tactical and strategic intelligence production breaks down. As an operational problem, however, it raises two very basic management questions.

MANAGEMENT QUESTIONS: What percentage of time and effort will be devoted to "strategic" requirements by "tactical" intelligence collection resources? Also, how will data base information be exchanged and maintained between these two levels?

3) The question of all-source intelligence integration is, as noted above, not so much a question of method but of structure. The structure which is currently being contemplated involves setting up all-source analysis centers at both division and corps levels. Aside from the possible question of redundancy involved in such parallel structures, some people have questioned the need for the division-level center -- seeing any divisional CEWI effort as one of collection management and reporting, not analysis. This critique also suggests that the focus of divisional intelligence efforts -- out to a maximum of 90 miles from friendly territory by doctrinal definition -- is, because of the speed of modern, mobile warfare, largely a function of combat information, not intelligence analysis.

MANAGEMENT QUESTIONS: At what level do we set up a dedicated structure for all-source intelligence analysis? Should it be a function of division, corps, or even an echelon above the corps?

4) The logic of combining electronic warfare and combat intelligence has

not been as obvious to some critics as it apparently was to the Ursano Commission. The SIGINT community in particular has done a good deal of mumbling into its collective beard about the alleged fact that this combination is one of "apples and oranges," and is, moreover, destined to come to no good for either discipline. They have, on a more reasonable level, questioned the propriety of devoting scarce resources to tactical, as opposed to strategic, missions. The response to this argument has been that there is no alternative to the presence of electronic warfare assets in combat units, and that CEWI provides a method for insuring the availability of these assets to the combat commander. A counter-argument to that response is that some strategic EW assets should remain permanently beyond the reach of any tactical command, possibly in the form of something like the present strategically-oriented Intelligence and Security Command.

MANAGEMENT QUESTION: Do we continue the present combination of electronic warfare and combat intelligence within the CEWI structure, or should we examine the possibilities for alternative arrangements of electronic warfare within the tactical environment?

Methodology/ideology.

1) The process of intelligence formation at the tactical level, as noted above, has been attended by some controversy over the question of acquiring data which is more appropriate to firing batteries than to intelligence analysis. In part, this quarreling is attributable to the fact that , until now, operational applications of the "intelligence cycle" have not included a clear recognition of the procedures whereby a certain

portion of the information collected is "bled off" and, where appropriate, passed to the firing batteries, with the rest of the data being processed for more leisurely comparison and analysis.[22] This ambiguity has also perpetuated the view in some sectors of the MI community that all surveillance assets should come under CEWI-imposed supervision.

MANAGEMENT QUESTION: Which targets, functions, and acquisition systems are more appropriate for the intelligence exploitation mission, which ones for fire direction and control -- and how can we tell the difference?

2) Deficiencies in the tactical exploitation of human-source intelligence or HUMINT, have been a source of some concern for those who argue that the new tactical intelligence architecture is dangerously dependent on information and data derived from technical systems, citing the extreme vulnerability of both airborne collection systems and EW assets in the face of identified Soviet capabilities. While the CEWI concept does allow for the use the more conventional HUMINT sources (interrogation of prisoners-of-war, reports from long-range patrols and observations of front-line troops) it does not provide a convincing place for these data in the all-source analysis system -- which is predominantly based on the mass data derived from the technical collection systems. Still other critics have noted that the counter-intelligence assets assigned to CEWI units, while theoretically capable of assuming a portion of the HUMINT collection mission, are for the most part committed to OPSEC support roles. Indeed, with the exception of interrogators (whose success obviously depends upon the availability of prisoners to interrogate), there are no units under the present CEWI concept which are dedicated to the positive collection

of human-source intelligence.

MANAGEMENT QUESTION: Assuming that we need it at all in a tactical setting, how do we procure human-source intelligence and what assets should we commit to this mission?

3) The question of whether the CEWI structure is adaptable for all wars in which the U.S. Army might find itself engaged is one which has been raised in a number of different contexts. The most pervasive critique, and probably the most controversial, was voiced in Military Review in an article in which an MI major suggested that the assumptions governing the technological approach toward warfare by FM 100-5 may have been too narrowly drawn. While not addressing the CEWI issue directly, he criticized the manual's acceptance of the idea that advanced military technology was the best way of defining one's future adversaries:

> We surveyed the world for an enemy and found, literally, ourselves. In a real sense, we have defined the relevant world, and the capabilities of our opponents in that world, in terms of our own perceptions of our own capabilities and limitations.... We may indeed have avoided the mistake of preparing now for the last war, but we may instead have committed a new error: preparing for a preferred war.[23]

Coming in early 1980 when the prospect of a war in the Persian Gulf looms as a real possibility, the thought forces consideration of the idea that perhaps our military intelligence base should be structured so that it can function acceptably in situations in which "low technology" dominates. The obvious examples of such conflicts are in insurgency conflicts, during which relevant intelligence targets are not the high-speed "movers, shooters, and emitters" of a European-based conflict but rather such non-quantifiable variables as ideology, infrastructure, and even religion.

MANAGEMENT QUESTION: Does the present CEWI structure make our military intelligence base more or less capable of fighting in a wide variety of conflicts with a minimum of adaptation?

Communications. Like the following area of resources, the problem of communications is a transcendent one and for that reason is handled here only in summary fashion. The CEWI organization, in fact, places unprecedented demands upon the tactical communications system with a quantum increase envisioned in every category of radio net: FM voice, high-frequency radio-teletype, and multi-channel. Equally unprecedented are the technological demands of making these communications secure from interception, interruption or simple destruction, given known Soviet capabilities for "radio-electronic combat." Indeed, a comparison of the "knowns" in both these categories appears to give an edge to the Soviet potential for targeting critical information reporting and processing links. Technological advances, such as those suggested in the fields of fiber optics and laser-based communications, offer some hopes of solution but not without an attendant degree of risk, expense, and most important, time.

MANAGEMENT QUESTION: To what extent will innovations in the architecture of the tactical intelligence reporting and processing system require parallel advances in secure communications to insure successful operation?

Resources. Every area of the CEWI structure carries a price tag in terms of personnel, equipment, training, and maintenance. While that is a truism, of course, for every other facet of military life as well, there is much to suggest that the Army has found even the testing phase of the new structure to be flawed by resource constraints. Particularly in the field

of personnel, where trained intelligence specialists are under strength in almost every category, the investment of 524 officers and men in the CEWI battalion seems somewhat excessive; when one considers that the suggested strength figure for the CEWI Group is over 2000 people, there is an obvious question as to the ability of the system to support the requirement at all. The technological investments required in communications, ADP systems, and software development have been mentioned above and need not be repeated here. Taken together, however, they raise the following issues as resource problems:

MANAGEMENT QUESTIONS: Is the proposed CEWI structure feasible in terms of the ability of the Army to provide resources to deploy it operationally as it is now envisioned conceptually? Is the CEWI structure too large and complex for the mission it was originally intended to perform?

Almost every defense-related question must be balanced against some kind of a cost/benefit equation that helps determine if it is "do-able" in terms of known resource availability. While that is certainly true of CEWI as well, there is also the matter of possible trade-offs between the tactical and the strategic intelligence missions. Assuming relatively constant amounts of dollars, of personnel, or of facilities, then there is the question of "how much is enough" in providing for the somewhat conflicting demands of each mission: when an innovation as ambitious as the CEWI structure is proposed, there is thus a de facto issue of who bears the costs of the incremental increase? Is it taken "out of hide" from other parts of the intelligence budget, must it be proposed to Congress as a supplemental budget increase -- or are there possibilities for economies of scope in streamlining

intelligence functions at both the tactical and strategic levels which may offset the additional costs incurred? While these questions are far more speculative than the management questions thus far developed, they do form the basis for an examination of the strategic side of military intelligence

MILITARY INTELLIGENCE AT THE STRATEGIC LEVEL: OLD IMPERATIVES, NEW REALITIES

In discussing the strategic realm of military intelligence, one immediately leaves the comforting presence of the Tables of Organization and Equipment, strength authorizations and advanced draft concept papers which surround the development of the CEWI structure. The strategic levels of military intelligence are notable for a contrasting lack of the same sense of purpose and direction which in fact characterizes the initiatives being taken at the tactical level. Whereas these initiatives may require more precise formulation of both purposes and resources, the strategic level seems largely devoid of any unified concept of future direction and effort.

In part, the inertia is attributable to the fact that the Army has yet to specify which command-and-control echelon will be placed above corps level -- historically either an army or a joint task force under an overall theater commander. This is not to say, however, that no such structures presently exist. In each of the Army's major overseas commands -- U.S. Army, Europe, or the Eighth Army in Korea, for example -- a staff structure along the basic lines shown in Figure I is present, with the G-2 function at this level being vested in a Deputy Chief of Staff for Intelligence (DCSI),

normally a two-star general. Each of these commands reports in turn directly to the Army Chief of Staff in Washington, who also has an Assistant Chief of Staff for Intelligence (ACSI); interestingly enough, the ACSI is also a two-star general and ranks below the deputy chiefs on the Army staff for operations, personnel, and logistics -- all of whom are three-star generals. These intelligence entities, however, are organized as staff, rather than line functions. While they maintain what are typically command reporting channels, they do not conduct intelligence operations per se.

The element which does conduct such operations is the Intelligence & Security Command (INSCOM), which was formed in response to one of the major recommendations of the Ursano Commission. Its functions include command-and-control of all non-tactical Army intelligence assets. This means that it is directly subordinate to the Army Chief of Staff and that it incorporates all strategic Army assets for SIGINT and HUMINT, including cryptology and counter-intelligence. In some sense, INSCOM is seen as a kind of evolutionary step towards a strategic-level CEWI organization, even though few people on the Army staff or anywhere else are prepared to be more specific. INSCOM elements overseas maintain reporting links to both INSCOM and to the theater commands to which they are attached but not assigned -- a situation which closely resembles some aspects of the pre-CEWI tactical intelligence organization. The information gathered by the various INSCOM elements -- particularly the SIGINT field stations -- is reported to national-level intelligence agencies such as the National Security Agency (NSA). While the Department of Defense only acts as an executive agent for NSA (which is considered a national-level resource), the Defense Intelligence Agency (DIA) is wholly subordinate within DOD to the Joint Chiefs of Staff. However the joint-

service positions of both agencies give them an important degree of influence in setting operational priorities and even outright intelligence tasking for all service intelligence agencies, particularly those nominally commanded by INSCOM. While the creation of INSCOM represents a new departure from previous practice, the general lines of strategic military intelligence collection have been in place since the early 1960's.

There is some evidence that this structure may be forced to respond to a variety of new pressures. The relationships of operational control versus nominal command remain somewhat ambiguous, and they have not been fully resolved by the creation of INSCOM. The changes being contemplated under CEWI also seem likely to force a more consistent approach in the line-up of tactical and strategic organizations. At a more profound level, however, there is a growing conviction that the existing strategic intelligence architecture may not be able to support the demands which will be placed upon it by new concepts in war-fighting doctrine in the mid 1980's. This idea stems from the concept that U.S. strategic nuclear doctrine has historically been based upon deterrence through threat of massive retaliation, even though amended by the idea of "flexible response." The strategic architecture of the intelligence community reflected this conception, since it was -- and is -- directed to perform most efficiently under peacetime conditions. If sub-nuclear conflicts should occur, the logic went, then the structure could be modified to meet whatever demands were imposed. Almost by definition, such a war would not be fought against the Soviet Union and, therefore, would not impose a direct threat to the United States -- hence time would allow for modifications. Refinements in nuclear warhead accuracy and effects have cast doubt on this construct, simply because they create more plausible scenarios for limited

nuclear wars. In such conflicts, time may not allow modifications of the intelligence base; more disturbing is the idea that national command authority facilities and the intelligence structure may themselves be likely targets for "decapitating" surprise nuclear strikes.

It is against this grim background that the outlines of a new strategic structure for the military intelligence base are beginning to emerge. The ACSI staff has recently circulated for draft comment a document entitled "Principles for the Employment of Army Intelligence," describing the total MI effort as "a single integrated system, but... decentralized in organization and management."[24] In describing the operational principles which tie the system together, their study makes use of an interesting matrix, showing the mix of intelligence disciplines (and the synergistic "multi-discipline" category) with sub-system activities conducted by each echelon of the system, from maneuver battalion to national levels. (A copy of their illustration is reproduced in Figure V.[25]) While the approach is highly conceptual, it is an important first step in viewing the entire military intelligence structure as part of an organic whole.

Equally interesting has been the appearance of the first draft of a new Army field manual specifying a tentative structure for the echelon above corps. This is the first hint, not only of what that organization will look like, but how its intelligence support will be structured. The organizational diagram reproduced at Figure VI shows that the keystone of this structure will be the Theater Army Intelligence Command (TAIC) subordinate to INSCOM in peacetime and to the theater commander in war. The TAIC will also direct the operations of one or more MI Groups (Command Support), which are tailored "to fulfill the intelligence requirements of the supported command and certain

overriding national intelligence requirements."[26] As the diagram also makes clear, these overriding national requirements are primarily the strategic applications of all three major intelligence disciplines, particularly HUMINT. Interestingly enough, this structure is organizationally set apart from the CEWI Groups supporting the tactical corps, even though there is a direct assumption that many of their operations will coincide.

This brief view of the beginnings of the strategic side of the military intelligence architecture is clearly not definitive, but it does suggest that we examine potential management issues from the perspective of three basic questions:

1) What is being done -- or contemplated -- at the tactical level that might be done as well or better at the strategic level?

2) What is not being done at either level that must be done in order to insure that the intelligence system works well under all conditions?

3) What functions, activities, or missions overlap between the tactical and the strategic levels, and could therefore be looked at for potential consolidation?

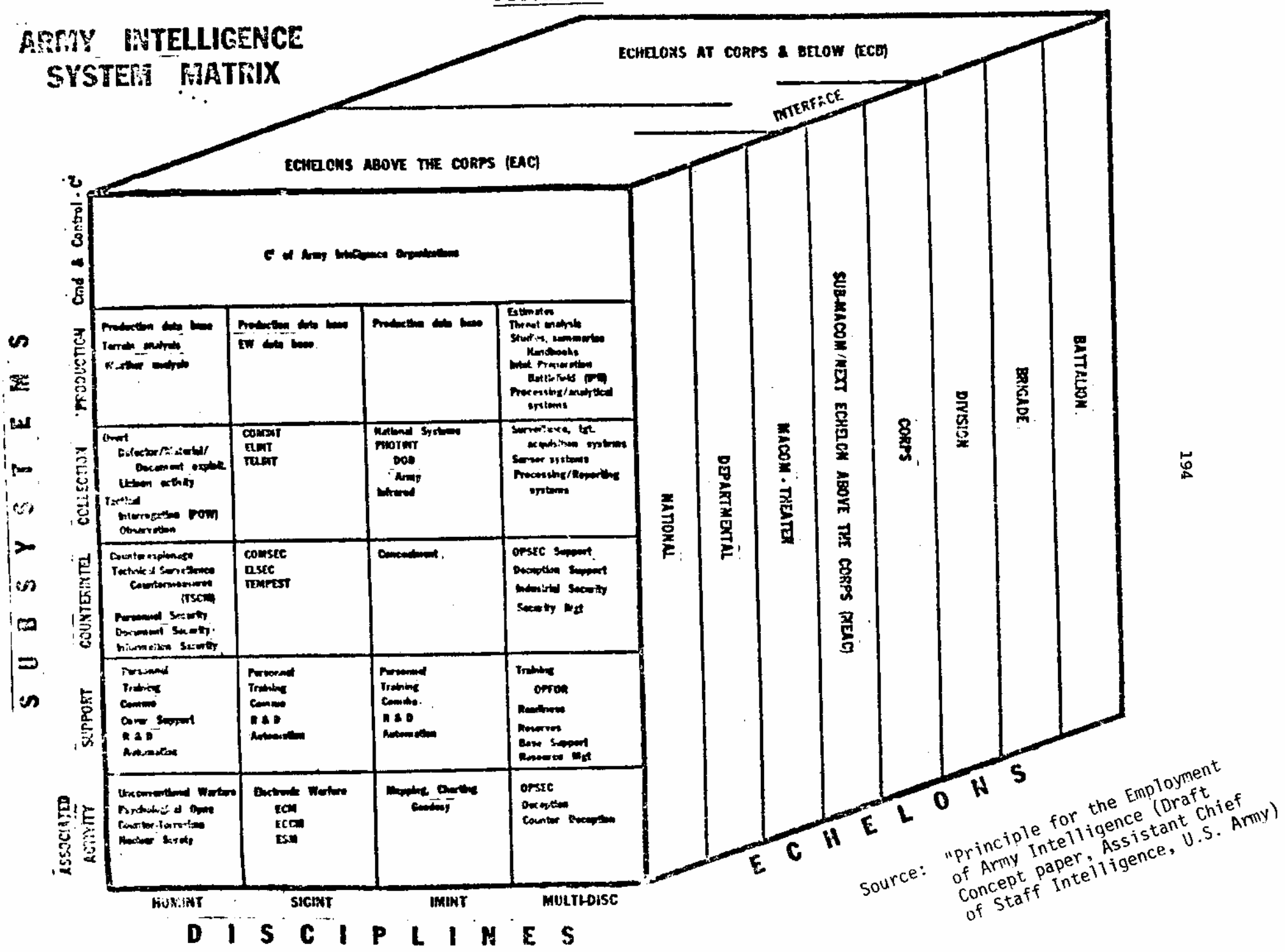
As in the previous section, we shall examine the same four areas of potential management questions: operational/technical, methodology/ideology, communications, and resources.

Operational/Technical

The three issues raised in this category in our analysis of the CEWI structure were the use of ADP systems, the exchange of data base information and the organizational level appropriate for all-source integration of

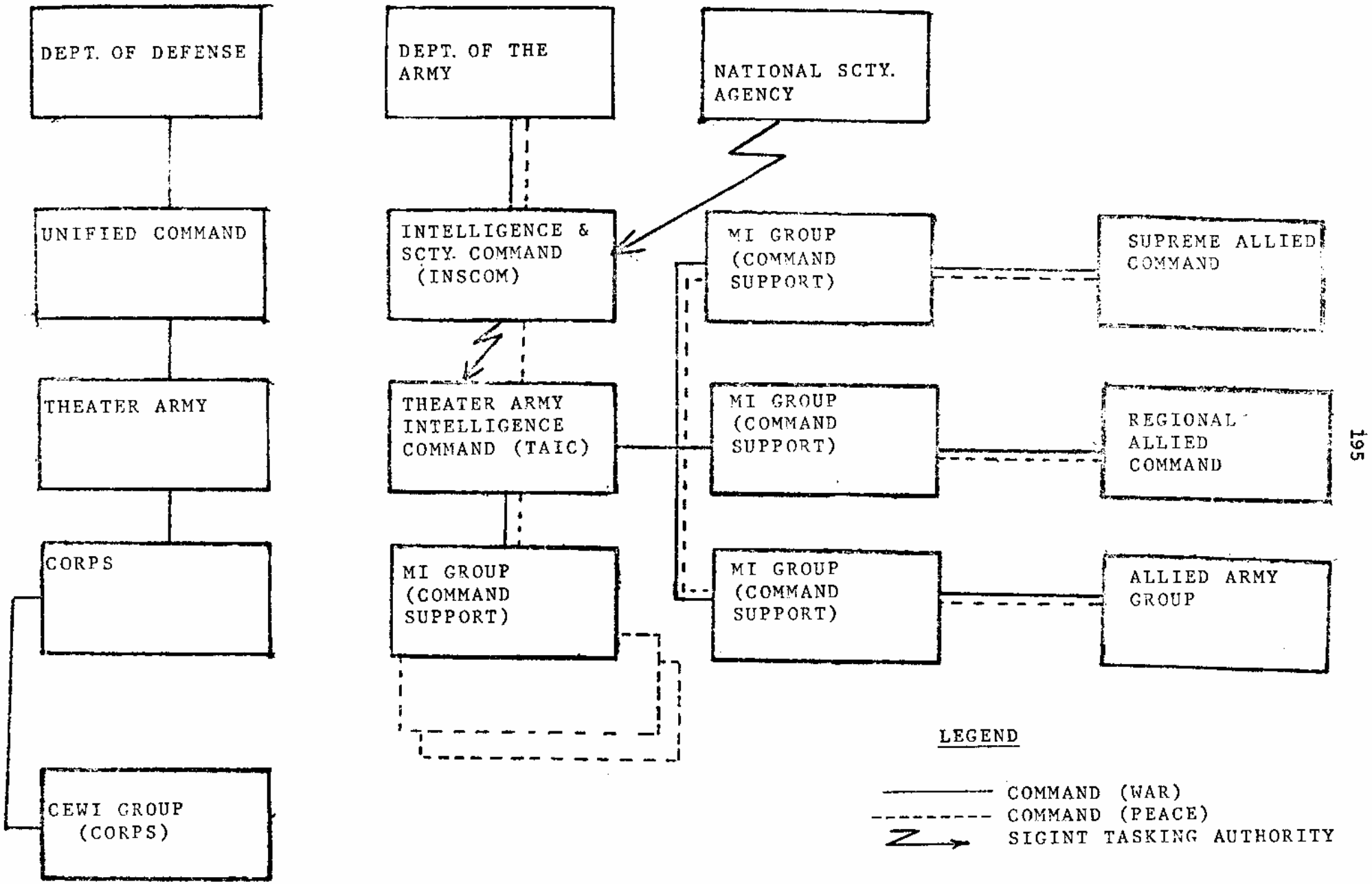
FIGURE V:

ARMY INTELLIGENCE SYSTEM MATRIX



Source: "Principle for the Employment of Army Intelligence (Draft Concept paper, Assistant Chief of Staff Intelligence, U.S. Army)

FIGURE VI: PROPOSED STRUCTURE OF STRATEGIC MILITARY INTELLIGENCE ORGANIZATIONS



SOURCE: FM 100-16 (Draft) Operations: Echelons Above Corps

intelligence. The suggested presence of the TAIC element as the primary link between the tactical and strategic echelons presents an interesting area for further study since there would appear to be some potential consolidation gains which might be realized in one or more of these three issue areas. Using the TAIC, for example, to consolidate what are now thought to be major ADP sections in each of the CEWI groups and battalions might be one potential solution to the problem of battlefield survivability, since the TAIC would presumably operate from more secure rear areas. Possibly it might also allow fewer ADP centers to be deployed and yet achieve the same level of operational flexibility. The problem of data base exchange might be considerably alleviated by the TAIC, if for no other reason than that it is far easier for a national intelligence agency such as NSA to provide data base information on a theater level than on a corps or even a divisional level. If data bases are being maintained with the pipelined specificity sometimes suggested for CEWI, there would be fairly impressive problems just in re-programming computers and other related equipment to adjust to the changes. A theater-wide data base greatly alleviates such a possibility, while possible also minimizing the communications channels needed to insure proper access to the national level. It is harder to assess whether the TAIC or the CEWI Groups or even the CEWI battalions should be the organizational focal point for all-source integration; the TAIC level stand out as one level which definitely should have that capability, the CEWI Group as a level which possibly could have it and the CEWI battalion as a level which possible can dispense with it and act primarily as a management and reporting channel. Here again there is a need for detailed further study and inputs from both operations specialists and force structure planners.

Methodology/Ideology

The basic issues raised by the CEWI structure dealt with the level of intelligence collection activity, the deficiencies in the tactical exploitation of HUMINT, and flexibility to fight in different scenarios with a minimum of adaptation. The TAIC appears to answer the need for insuring that strategically significant information is collected, since it is set up organizationally to answer the intelligence needs of a strategic-level commander. It does not address, of course, the question of resource allocation between the TAIC and the CEWI organizations. The need for effective HUMINT is recognized by the TAIC as a function which is appropriate for administration by the strategic as opposed to the tactical level. While the concept is hard to dispute in a doctrinal context and the proposal to create a HUMINT capability is voiced in apparent good faith, the problem of how to set up an operationally effective tactical HUMINT system cannot be wished away with a simple declaration of intent. One would wish to see a much more precise outline of the resources and missions of such a group, together with a better idea of how their information will be collated with the results of technical collection systems. Until then, judgment must be withheld on this point. Similarly, the thinking in the new manual and the primacy which is attached to the idea of tailoring specific wartime scenarios is a welcome step away from the simplistic notion of FM 100-5 which seemed to suggest that "one size fits all." The danger here is that the new manual stops short of requiring Army commanders to test out these new "tailored" structures prior to having to deploy them

for potential combat situations. Consequently, there is a need for the strategically tailored intelligence units to be tested and evaluated together with the tactical organizations they are meant to be supporting in the field.

Communications

The transcendent problem of communications will be as much a problem for the TAIC organizations as it is for any other entity of the intelligence system. Moreover, this is the kind of problem which is not solved by organizational planning, but rather by the application of state-of-the-art technology. Where the planning does come in, however, is in figuring out with some precision who communicates with whom. In this regard, the CEWI Group is clearly incapable of performing what it touted as its ability to act as the primary strategic-tactical communications link. Its status as the net control for an extensive hook-up of tactical reporting and processing stations is a large enough mission precisely as it stands now. Adding the greater responsibility of communicating with the national-level commands is insupportable purely on organizational grounds; when one also considers the likelihood of the EW challenges which will be faced by the tactical radio system, it would clearly be unwise to place all of the communications "eggs" in this one basket. Unfortunately, specific information is lacking on how the TAIC-level units might be configured to fill this gap or how they would be linked to the CEWI all-source analysis system, or how redundancies might be built into the reporting system between these entities to insure a greater degree of survivability. Similarly, there is also a disconcerting lack of proposed solutions to insure that the link between TAIC and national levels remains open for communications under all conditions, and in particular with respect to the

likely challenges posed by various methods of interrupting or degrading satellite transmissions. In this area, more work needs to be done in harnessing present, near-term, and long-range communications capabilities to the kinds of organizational entities which we expect to have in the field during those time sequences.

Resources

The CEWI structure is, as has been seen, heavily dependent on a wide variety of resources, most notably personnel and equipment. The TAIC and its subordinate MI Groups for Command Support would appear to share the same characteristic. The relatively hazy outlines of both the CEWI Group and the TAIC concept do nothing to alleviate the possible ambiguities of resource constraints noted earlier. In fact, the very suggestion of the addition of strategic-level intelligence units heightens the importance of this point. There are some obvious economies of scale which, without much intellectual effort, seem like reasonable starting points for organizational pruning. If, for example, we have an MI Group for Command Support, do we also need to have full-blown CEWI Groups as they appear on paper at present? Are these possible equipment savings which would result from consolidating some strategic EW assets at theater level? The problem here is that strategic and tactical structures have not been analytically paired either to each other or to the areas of likely resource constraints. Until that effort takes place, this aspect of our force planning can only be described as speculative.

PULLING IT TOGETHER: SOME SUGGESTIONS

This study has attempted to assess the management side of the effort by the military intelligence community to create a new structure which will enable it to better support the United States Army. It has described the organizational and technological milieu which has compelled the changes through a series of action-forcing events. It has also identified specific management issues which have thus far emerged from the experience of building a new tactical intelligence structure, and finally, it has paired these issues with the conceptual outlines of the new strategic intelligence architecture. It has thus been able to identify specific issues that need to be examined further and suggested specific areas which required more detailed and analytical inputs. There is no need to repeat any of these findings here or to make absolute recommendations based on their tentative implications.

There is a need, however, to suggest some important lessons that should be learned from the process that has emerged thus far, lessons which have a great deal to say about the deficiencies that have been identified here. The first and most basic point is that the design of the tactical structure has been fundamentally flawed because it has been considered in isolation from the requirements of the intelligence system as an organic whole. This misconception has led to great confusion over "who does what and with which and to whom." It has also led to various parts of the system acting out of perceived wants in their own bailiwicks, and not out of demonstrated needs which the system as a whole must fill if it is to be effective. Consequently, there are some organizational monstrosities mixed in with a number of solid structural reforms.

The second point is that the pace of development of the military intelligence architecture has been strikingly uneven, without an overriding concern for time-phasing development in a number of critically related areas. One looks in vain for a critical path network, a time-line, or even an overall developmental strategy. In this study, major problems have been identified requiring further inputs in the areas of communications, logistics, personnel, and equipment--to say nothing at all about the equally pressing matter of budget and fiscal constraints. If the intelligence architecture should be viewed as an organic whole, so should its developmental problems, unless the entire exercise is to be nothing more than a "paper drill" to do what seems politically expedient.

Finally, one cannot emphasize strongly enough that the Army needs to test out its putative intelligence structures in environments that are more intellectually demanding than the austere plains of Fort Hood, Texas. While there are, of course, good reasons for fielding these units in a tactical setting, this should be the last act in a drama that should have started in the more conceptual realm of war-gaming and simulation. In examining the progress of the CEWI battalion, for example, it is difficult to suppress the notion that it represented a "rush to judgment" in which the result was predetermined. A more productive approach is suggested by some of the procedures now operative in testing out the conceptual limits for advanced weapons systems: essentially, capabilities are designed against a variety of threats and scenarios. The resulting package is capable of meeting the threat, yet remains systematically

coherent. Surely our military intelligence system, as a potential weapon in its own right, could profit from the same sort of approach.

NOTES

1. General Omar Bradley, A Soldier's Story (New York: Henry Holt & Company, 1951), p. 33.

2. These achievements have been highlighted in recent years by several authors. The classic accounts of counter-intelligence and deception are contained in J. C. Masterman's, The Double-Cross System (New York: Avon Books, 1972) and Anthony Cave-Brown's Bodyguard of LIes (New York: Harper & Row, 1975). The Ultra Secret by F. W. Wintherbotham (London: Weidenfeld & Nicolson, 1974), presents the story of Allied signals intelligence against Germany during World War II.

3. Carl Maria con Clausewitz, Vom Kriege (On War), "Information in War." Reprinted in Clausewitz on War, ed. R. A. Leonard (New York: Capricorn Books, 1967), p. 83.

4. See William Manchester, American Caesar: Douglas MacArthur 1880-1964 (New York: Dell Books, 1979), pp. 684-686. Actually the case can be made that MacArthur took the "intelligence" point of view in planning the Yalu Landing, since he opted for surprise in the face of overwhelming operational obstacles.

5. Lieutenant General Harry W. O. Kinnard, "Narrowing The Intelligence Gap," Army Magazine (Vol. 19, No. 8), August, 1969, p. 22; cited in The Evolution of American Military Intelligence, by Majors M. B. Powe and E. E. Wilson, U.S. Army Intelligence Center & School Supr. 02520, Fort Huachuca, Arizona, May, 1973, p. 120.

6. Two of the classic accounts of this war--both of which are considered required reading for intelligence officers--are The Yom Kippur War by the Insight Team of the London Sunday Times (Garden City, New York: Doubleday & Co., 1974) and Chaim Herzog's, The War of Atonement (Boston, Little, Brown & Co., 1975).

7. U.S. Army, Field Manual (FM) 100-5 Operations (hereafter FM 100-5), Headquarters, Department of the Army, Washington, D.C., July 1, 1976, p. 1.

8. Ibid., p. 2-2.

9. Ibid., p. 2-6.

10. Ibid.

11. Ibid., p. 2-14.

12. Ibid., p. 2-27.

13. Ibid., p. 7-2.

14. Ibid. pp. 7-2 & 7-3.

15. A most perceptive article on Soviet Army doctrine and capabilities in the field of electronic warfare has recently appeared in the public domain. See Major Barney F. Slayton, "War In the Ether: Soviet Radio-Electronic Warfare," Military Review (Vol. LX, No. 1) January, 1980, pp. 56-68.

16. Summarized by the U.S. Army Intelligence Center & School, "Draft Operational and Organizational Concepts: Combat Electronic Warfare and Intelligence Group," February 27, 1980, Fort Huachuca, Arizona, p. 8.

17. A surprising amount of controversy developed over the name "CEWI" itself, leading one former CEWI commander to comment: "The blend of soft consonants and vowels provides a sound which tends to rattle around in the mouth. It is not sharp or crisp, like Ranger! or Airborne! It was observed that any unit referred to as a CEWI battalion would be forced to make a strong and vigorous effort for acceptance in a tactical unit." Lieutenant Colonel Don E. Gordon, "The CEWI Battalion: A Tactical Concept That Works," Military Review (Vol. LX, No. 1), January 1980, p. 7.

18. Lieutenant Colonel William E. Harmon, "CEWI Battalion Update," Military Intelligence Magazine, U.S. Army Intelligence Center & School, Fort Huachuca, Arizona, April-June 1978, p. 38.

19. LTC Don E. Gordon, op. cit., p. 8.

20. Brigadier General Albert N. Stubblebine, III (former commander U.S. Army Intelligence Center & School; currently commander, U.S. Army Electronic Research & Development Command), "C31 For Automated Focus On The Intelligence Picture," Army Magazine, March 1979, pp. 33-34.

21. Ibid.

22. An illustrative analogy can be made here to the operation of an automatic weapon. Once the cartridge is fired, expanding gases propel the bullet down the barrel and give it both velocity and long-term guidance. A portion of the barrel pressure, however, operates the reciprocating piston of the chambering mechanism to perform the more immediate task of loading the next round to be fired. In terms of effectiveness, both functions are vital. So must the information collected by the tactical collection process be exploited for both long-term guidance (the intelligence process) and short-term fire control.

23. Major John M. Oseth, "FM 100-5 Revisited: The Need For Better Foundation Concepts?", Military Review (Vol. LX, No. 3) March 1980, pp. 15-16.

24. U.S. Army, "Draft Principles For The Employment of Army Intelligence," Headquarters, Department of the Army, undated, Washington, D.C., p. 2.

25. Ibid.

26. U.S. Army, Draft Field Manual 100-16, Operations: Echelons Above Corps, Deputy Chief of Staff for Operations and Plans, Headquarters, Department of the Army, Nov. 1, 1978, Washington, D.C., p. VI-5.

BIBLIOGRAPHY

Bracken, Paul. "Command & Control for a Long War." Air Force Magazine (April, 1980), pp. 50-54.

Bradley, Omar N. (General-U.S.A.). A Soldier's Story. New York: Henry Holt & Co., 1951.

Cave-Brown, Anthony. Bodyguard of Lies. New York: Harper & Row, 1978.

Clausewitz, Carl Maria von. Editor R. A. Leonard. Clausewitz On War. New York: Capricorn Books, 1967.

De Wilde, David A. (Lieutenant Colonel - U.S. Air Force). A Command And Control System For The NCA: What's Needed. Air War College Report No. 5226. Maxwell Air Force Base, Alabama. April, 1974.

Gordon, Don E. (Lieutenant Colonel - U.S.). "The CEWI Battalion: A Tactical Concept That Works". Military Review, LX (January, 1980), pp. 2-11.

Harmon, William E. (Lieutenant Colonel-U.S.A.). "CEWI Battalion Update". Military Intelligence Magazine (U.S. Army Intelligence Center & School, Fort Huachuca, AZ.). (April-June, 1978).

Herzog, Chaim. War of Atonement. Boston: Little, Brown & Co., 1975.

Latimer, Thomas K. "U.S. Intelligence and the Congress." Strategic Review. (Summer, 1979), pp. 47-56.

London Sunday Times Insight Team. The Yom Kippur War. New York: Doubleday & Co., 1974.

Mahaffey, Fred K. (Major General-U.S.A.)."C3I for Automated Control of Tomorrow's Battlefield." Army Magazine. (March, 1979), pp. 26-31.

Manchester, William. American Caesar: Douglas MacArthur 1880-1964. New York: Dell Books, 1979.

Masterman, J.C. The Double-Cross System. New York: Avon Books, 1972.

Oseth, John M. (Major General-U.S.A.). "FM 100-5 Revisited: The Need for Better Foundation Concepts?" Military Review (Vol. LX, No. 3) March 1980, pp. 15-16.

O'Shea, Cornelius J. (Lieutenant Colonel-U.S.A.). "Tactical Intelligence Development and the Utility of Force" (Article prepared for forthcoming edition of Military Review).

Powe, Marc B. (LTC-U.S.A.) and Wilson, E.E. The Evolution of American Military Intelligence. U.S. Army Intelligence Center & School, Fort Huachuca, Arizona, 1973.

Slayton, Barney F. (Major-U.S.A.). "War In The Ether: Soviet Radio-Electronic Warfare." Military Review, LX (January, 1980), pp. 56-68.

Stanford Research Institute. A Retrospective Look At Some Of The Basic Issues Connected With National Command, Control and Communications. Menlo Park, CA, 1980.

Stubblebine, Albert N. III (Brigadier General-U.S.A.). "C3I For Automated Focus on the Intelligence Picture." Army Magazine (March, 1979), pp. 31-35.

U.S., Army. "Draft Army Tactical Intelligence Concept." Headquarters, U.S. Army Training & Doctrine Command. Fort Monroe, VA. November 26, 1979.

U.S., Army. Draft Field Manual 100-16, Operations: Echelons Above Corps. Office of the Deputy Chief of Staff for Operations and Plans, Department of the Army, Washington, D.C. November 1, 1978.

U.S., Army. "Draft Operational and Organizational Concept: Combat Electronic Warfare and Intelligence Group". U.S. Army Intelligence Center & School, Fort Huachuca, AZ. February 27, 1980.

U.S., Army. "Draft Principles for the Employment of Army Intelligence." Office of the Assistant Chief of Staff for Intelligence, Department of the Army. Washington, D. C. (undated).

U.S., Army. Field Manual 100-5, Operations. Headquarters, Department of the Army. Washington, D. C. July 1, 1976.

Wintherbotham, F. W. The Ultra Secret. London: Weidenfeld & Nicolson, 1974.

5. INTELLIGENCE AND INFORMATION SYSTEMS IN THE DEPARTMENT OF STATE/FOREIGN SERVICE

David C. McGaffey

TABLE OF CONTENTS

INTRODUCTION

Characteristic of any complex organism is a sensory system for receiving and processing information about the outside world as a prerequisite for action or reaction. For the organism known as the U. S. Government, the State Department and the Foreign Service serve as one of the government's sensory systems in its role as a collector and analyzer of information about the activities of foreign states and peoples. In advanced organisms, the sensory system also functions as a filter, processing and transmitting only that portion of information deemed of importance to the organism--e.g., the eye "sees" everything in an average 140° arc in front of it, "perceives" only the pattern it is adjusted to, and "notices" only dynamic deviations from that pattern unless concentrating.[1] Similarly, the Foreign Service "sees" the entire world and its activities, "perceives" only those elements considered relevant to the U.S. goals, needs, and interests, and "notices" only those changes considered likely to have a positive or negative effect on those interests. To do otherwise would render it ineffective. One definition of schizophrenia is the inability to filter out irrelevant information input, thus causing a paralysis of the ability to choose.[2] Similarly, in organizations, information overloads "delay communications and decisions, make them erratic or wrong, and may result in their not being made."[3]

Thus, an essential characteristic of an information collecting and processing system such as the Foreign Service is its capacity to filter out irrelevant information. It follows that an equally vital characteristic is the ability to accurately distinguish the relevant from the irrelevant at each filtering step. An individual without this ability is called psychotic. An organization without this ability is certainly ineffective, and probably

pathological in terms of the overall organism or society it serves. In a dynamic organism such as the U. S. Government, where national interests, needs, and goals are subject to continuous change, the system of information collection and processing must then be characterized by a two-way information flow, with exterior information being multiply-filtered as it is passed up through the structure, and with information about relevance being continually passed down through the structure to adjust the filters to changing perceptions of U. S. interests.

The structure of the State Department/Foreign Service information processing system evolved over a period of time during which the U.S. was both so relatively isolated from foreign events and so relatively strong that the impact of foreign events was weak. Even two world wars had done no more than to confirm a necessity for the U. S. to be interested in what the rest of the world was doing, without altering the basic perception that U. S. actions could be determined largely in isolation from foreign affairs. Since World War II, however, the growing economic interdependence of the U. S. with the world--deriving to a great extent from the U. S. role in post-war economic reconstruction of Japan, Germany, Italy, and their erstwhile possessions; the growth of the U.S.S.R. as a rival socio-economic model; and the increasingly real threat of destruction from the development of nuclear weapons technology--has created a necessity for an improved capacity in the U. S. to understand and react to foreign actions and events.

The traditional Foreign Service intelligence function, defined in a time when events had little short-term impact on the U. S., has put little importance on the quality of speed in processing information. However, since for most of its existence the Foreign Service has been required to <u>persuade</u>

decision makers that they should take foreign developments into account, it has placed great importance on the quality of accuracy. The organization of this system--and the defined functions of its components--thus reflects the purpose of the system: to provide careful, accurate, multiply-checked and filtered analyses of a broad base of information in order to guide decision makers in those areas with foreign, or joint domestic-foreign, implications. Faced with a changed world--where almost all U. S. decisions now have foreign implications, where the amount of foreign information affecting U. S. decisions and interests is increasing daily, and where the value of time has become equally as important as accuracy in making decisions--this system has tried to adapt.

The almost total substitution of telegrams for dispatches, the multiplication of posts abroad (and of areas of concern to those posts), and the almost constant personnel reorganizations in the Department and the Foreign Service attest to the attempts at adaptation. It appears, however, that these are not enough. Following the fall of the Shah of Iran, the White House declared that there had been a "failure in U. S. intelligence." As each element of the system examined its performance of its assigned function, the response to the White House was indignation, as no failure of any component could be determined. The system had worked as it was designed.

However, given that the purpose of the system is to provide decision makers with the guidance needed for correct decisions, and given that incorrect decisions had been made, then the system has failed either in developing the correct information or in its ability to guide the decision makers. If the components fulfilled their functions, then it is necessary to refine the system, assigning new functions to the system elements or, at minimum, to re-

examine the system to determine how the various elements interact, finding a way to improve system performance.

One model of a different system--Command, Control, Communications, and Intelligence (C^3I)--has evolved from a different history in military usage. The State Department has adapted this system in part for crisis management in the Operations Center of the Office of the Secretary of State (the Ops Center). This paper will examine those two existing systems, their elements and the specific functions of the elements, to see whether either, or an amalgam of the best of each, can best serve as the model for the information collection and processing system which the U. S. Government needs to survive in a new age of interdependence.

COMMAND, CONTROL, COMMUNICATIONS AND INTELLIGENCE

C^3I can be defined as a complex system providing intelligent centralized management of multiple action/reaction elements to achieve an optimum response to constantly varying external stimuli to promote objectives which are themselves subject to slower, evolutionary changes. It usually requires a two-way information/communication flow. Its origins are military, and it was first defined as the system which allowed a senior military command the flexibility to deviate from pre-set tactical plans to take advantage of current information from the battlefield, by controlling the action of all tactical units during the course of action. As it became obvious that the needs of the tactical commander during action are not significantly different from the needs of the National Command Authorities in peace and war, and as the changing nature of war with the spread and development of nuclear weapons made the National Command Authorities the actual tactical commander in the

event of a nuclear exchange, C^3I became the name for the system through which the National Command Authorities manage all components of the national government, domestic and foreign, military and civilian, during peacetime, war, or any intermediate stages.

U. S. C^3I as a single, unified system does not yet exist, and may never come to exist. Currently, there exists a military-nuclear-tactical C^3I of untested reliability, and a peacetime military-civilian C^3I of demonstrated capability (but untested reliability in case of nuclear war). While integration of these systems appears desirable, it is necessary to study closely the necessary elements of such an integrated system so as to avoid expensive and dangerous errors.

CENTRALIZATION AND CHANNELLING--VALUES AND DANGERS

Any complex C^3I system is an attempt to resolve an inherent conflict: the command authority requires speed, both in acquiring information and in disseminating instructions; it also requires accuracy, both in the information it receives and in the transmittal of instructions. The basis for the conflict between these two goals lies in the fact that complex systems appear to be counter-intuitive, i.e., in the face of external stimuli which throw the system into disequilibrium, the "obvious" reaction in most cases will not in the long run restore equilibrium, but will tend to exacerbate the problem. For example, urban studies in the U. S. have shown that for a city with a housing imbalance caused by inadequate or substandard housing, urban renewal projects to build or refurbish housing will attract new immigrants, leaving the city with an even greater housing imbalance.[4] Thus the command authorities cannot be satisfied with speed in reporting incidents and carrying out

orders; they must require careful and in-depth analysis of events before they act, and such analysis consumes time. On the other hand, if they insist on complete analysis of every event, they find the world refuses to stand still and wait, so their chances for action pass them by. Any C^3I system must make a trade-off between these two objectives. The means by which this trade-off is made is by relative emphasis on either centralization or on channels.

CHANNELS--INTERACTIVE CHAIN LINKS

The Nature and Purpose of the System

The traditional bureaucratic system is a hierarchical system of specialization with specific links of authority and responsibility defining the flow of work, product, or (here) information through the system. The Foreign Service bureaucracy shares most characteristics with other bureaucracies with some significant differences. One such difference is that it is, except at the highest (policy) levels, simultaneously a hierarchy and a collegial system. Each member of the intelligence system is an officer, individually commissioned and sworn to uphold and better the interest of the United States. With its "rank-in-man" concept, it consciously separates its authority structure from responsibility, which is considered to be equally shared, in theory if not in practice. It coexists with a more rigidly hierarchical structure of support personnel, but its own job levels are considered to reflect experience and individual capabilities, rather than intrinsic differences between jobs. A related difference between this system and most other bureaucracies is that the specializations of the different levels are not in work requirements, but in scope of work. While the scope for each individual varies, the information collection and analysis, as well as the goal, remain roughly the same for each level. A primary function of authority is to define

the scope of work for the level immediately lower in the hierarchy. However, the individual also self-defines his own scope of work, and receives information from others at the same level, from those outside the system, and from known individuals at other levels in the system--all of which influences the scope of work. When the authoritative scope-of-work differs from the individual's definition, it is a shared responsibility of superior and inferior, as colleagues, to amend one or the other definition until they correspond.

A major role of the State Department/Foreign Service bureaucracy is the collection and analysis of foreign intelligence, primarily gathered from and by human resources. Its objectives are to analyze foreign events having effects on U. S. interests, to report this information to policy makers after analysis, and to recommend courses of action by which the U. S. can benefit from favorable events and mitigate the effects of unfavorable ones. Its task is difficult, involving understanding of alien cultures and thought-patterns and interpreting them in terms of U. S. culture. As the system is designed to emphasize accuracy over all, when U. S. foreign policy appears successful, it is assumed that the Foreign Service is merely doing its job; when foreign policy is seen as failing, the system and/or individuals in the system are blamed. For this reason, and because success or failure can be determined only ex post facto, the system encourages caution. Judgments become liberally salted with qualifications, equivocations, exceptions, and alternatives. While this makes them less useful to higher levels (which will also try to cover themselves), it enables the analyst to demonstrate some degree of accuracy, especially as circumstances have a habit of changing during the long time between the analyst's typewriter and the policy maker's desk.

To protect himself, "super-crat" invents a "multiple option pocket

computer . . . to consider all alternatives and every variation of any situation imaginable. The object . . . is to sneak everything into cable traffic. That way, no matter what happens, Ambassadors and bureaucrats can claim -- 'I predicted that. . . .' When everything is over and done, you just toot your own horn by sending in a one-liner, referencing your only telegram that was on the mark."

The system also relies on access to (and the good will of) the policy makers, so it has a tendency to avoid distressing them by reporting bad news. The Foreign Service remembers the fate under Senator McCarthy of the "China Hands" who correctly forecast the success of Mao-Tse-Tung; so reports tend to emphasize the positive.

Finally, as stated above, the system places great emphasis on accuracy, and frowns on speed, which is seen as evidence of "hasty and unconsidered judgment."

Thus we can examine this system. For simplicity's sake, while the number of levels varies from area to area, I will examine a channel of only five elements: a field officer; a field director; a department contact; and a departmental principal who reports to the National Command Authority.

The field officer is the system's prime intelligence collector. His function is to gather information about the local situation through reading, personal observation, and contacts with individuals, and to make primary assessment as to the accuracy and relevance of the information to his goals and to provide analysis of that information as it relates to U. S. interests. His scope derives from policy guidance he receives from the field director but is largely self-determined within the boundaries of his resources and available information. His resources are: (a) his personal background,

language facility, knowledge and understanding of both the local history and culture and U. S. history and current interests; (b) his local status, derived from his official position and the status of the U. S. in his post of assignment, his predecessor's and colleagues' relations with local contacts, and (c) his available time. He contributes to the system both reporting of raw information and analysis of that information as it relates to the needs of the system. In addition, he consults with the field director when his perception of local events calls for a different scope of work than was directed, influencing not only his own and other field agents' scopes, but also the scope-of-work of the field director.

While there is a range of personal abilities making the officer more or less effective in his job, the selection and retention process should ensure that all officers fall within an acceptable range of competence. However, the field officer's understanding of the system's requirements (current and long-term U. S. interests) is critical to the value of his performance. As a foreigner studying an alien culture, he inevitably must focus on only a few matters if he wishes to understand them properly. He will select his areas of focus based on his understanding of what is important to U. S. goals. To the extent that his understanding is incorrect, incomplete, or uncertain, his selection and focus will be inappropriate to those goals. Moreover, his analysis, relating his information about those selected areas to his perception of U. S. interests, will be even more distorted if his perception is awry. He reports to, and receives his primary guidance on current U. S. interests from his principal officer or mission director.

The field director (ambassador, consul general, mission director) has direct contact with Washington and is responsible for the direction of a

field staff. (There may well be several layers between him and the lowest level field officer, but these merely duplicate divisions shown here.) His function, in addition to that of a field officer, is to direct his staff in their collection of information, to guide them in their analysis and reporting, and to perform independent analysis of their information, as well as information he might independently receive because of his rank and status. His scope is to collect all the information in his area vital to U. S. interests, to organize it, and to present integrated analyses of the relation the country of his assignment has to U. S. interests in the region and worldwide. His specific scope is derived from guidance from Washington and his staff's understanding of the local situation. His primary resource are his staff of field officers and their reports. He acts as a filter, directing his staff towards those areas which, in his understanding, are of primary importance to the U. S. within the limits of available manpower resources. In both his staff direction and his own analyses, the value of his efforts is directly affected by the accuracy of his understanding of U. S. goals and objectives. He reports to and receives guidance from, through intermediate channels in most cases, an assistant secretary, his department contact.

The department contact, normally an assistant secretary in charge of a geographic bureau, is the primary link between the policy makers and the information gatherers. In routine matters, he is the command authority, making policy decisions affecting his geographic region. In other matters, he is the filter, determining which information is of national consequence, and referring it upward. He is in direct contact with the secretary of state, and receives policy guidance from him. His scope, U. S. interests in a geographic area, is defined from that guidance, by guidance upward from his field directors, and personally through his background and contacts with

others within or outside the system. At this level, it is clearly impossible to focus on more than a tiny percentage of events in his area.

His goals are to integrate information received from his posts abroad and his staff within the department, to determine how that information affects U. S. interests, and then either to make decisions or to analyze that information of national importance in order to guide the decisions of the Secretary or the National Command Authorities. His resources are his posts abroad and the staff of his geographic bureau and of other analytical offices within the department. His instructions to the field directors constitute their primary guidance as to current U. S. goals and objectives; and, by focusing their attention on the indicated areas, perforce restrict their ability to examine other matters. Since the information derived from the field, in turn, determines his decisions and guidance to the secretary, his utility depends essentially on how well he understands U. S. current and long-term interests, which depends on his contact with the Secretary and other senior officials.

The department principal, the Secretary of State, is the principal advisor to the President on foreign affairs. At this point in the chain, he is not necessarily expected to have foreign expertise, but rather to have wide familiarity with the domestic political and economic situation, especially as it relates to the rest of the world. His function is to advise the President on interactions with the world: what U. S. actions are most likely to elicit desired foreign responses, what foreign events require a U. S. reaction, and what the domestic effects will be of the continuing international interreactions between states. Except on those issues where the President has strong personal views, the Secretary will be, in fact, the designer and

drafter of most statements of U. S. interests, goals, and objectives internationally, but he is dependent on his understanding of the President's wishes to ensure that any such statement will not conflict with the President's own goals. He is the ultimate filter; he determines what State Department information will reach the President, and ensures that the volume which does so is strictly minimized. In most events, he makes the ultimate decisions, alone or in consultation with his Cabinet colleagues. His resources are the staff of the State Department and the Foreign Service abroad, and the presidential powers and authority specifically or customarily delegated to him. As he is not usually a foreign expert, he is totally dependent on information received from his staff, and filtered in great measure before he sees it. If he is to have the information he needs for his decisions and his advice to the President, he must ensure that his staff clearly understands the issues and interests that he wishes to focus on, and his staff, who in the aggregate are the nation's expert on foreign affairs, must ensure that he becomes aware of, and focuses on, new issues as they become important to U. S. interests.

The National Command Authority, the President, must--within the constraints of the Constitution and law with the advice and (when required) consent of Congress--set the base goals and priorities for the U. S. government. He must select a Secretary of State who will fully understand those goals, and who will advise him on foreign affairs as they affect those goals. On matters of national importance, he must make decisions (and have those decisions carried out) through means up to and including war. In the current military situation, however, it must be a primary goal to avoid war whenever possible.

INTERACTION, FEEDBACK AND TRUST

As is clear from the above, this system of human intelligence about foreign affairs is essentially a process of filtering and refining--and of focused analysis. No system will allow for complete understanding of all aspects of the rest of the world, but this one does have the capacity to satisfy most needs. Except at the top, there is generous redundancy which provides a rough cut at accuracy analysis. Each level of each channel filters (both from personal conviction and from guidance from superiors) and sends information upward--both in response to guidance and in response to individual perception of importance. Each level ideally will also serve as a storage point for non-transmitted information (an institutional memory) so that as events, needs, and goals change, newly relevant information can feed through the chain from the filtration point rather than from the origin again.

CHANNELLED REPORTING AND ANALYSIS

In the direct channel, it is essential that the same means be used both for passing instructions down and passing information up. Only then can there be in each paired link a proper feedback, eliminating any misunderstanding about what is desired (whether that which provided fills these needs, and whether something in addition is needed or submitted). If the system attempted to pass down a total understanding of all the needs, interests, goals and desires of the President and the Secretary to each field officer, the system would exhaust its time and energies in this task. Instead, a similar filtering process works on the down side, but a partial understanding, as circumstances change, has its own dangers. Thus, a constant interaction and feedback process is essential for effectiveness. At the same time, it

must be recognized that the mere act of conversational feedback is insufficient. In a closed system, there will be personality conflicts, promotion games, and bureaucratic squabbling. Withholding or distorting information is a major weapon in such games and will destroy the value of feedback. What is required is the element of trust--at least on direct channel exchanges; the superior must accept on trust the competence, reliability, and professionalism of the informant, while the informant must trust the guidance and criticism of the superior. In the absence of trust there is either enmity or indifference. If enmity, one side will deliberately distort the exchange in order to make the other look bad. This, fortunately, is rare. In the much more common case of indifference, the exchanges, guidance, and feedback will be pro-forma with each providing the other with what he thinks the other wishes to hear. Because of uncertainty, there is a tendency, over time, for each to push the frontiers of the others' "wishes" until the exchange is not based at all on reality, but totally on the game. Nothing could be more destructive to the accuracy and efficiency of the system. With trust and constant feedback, however, this system is capable of generating extremely accurate information and analyses, as each member concentrates on his own area of expertise.

CROSS-, UP-, DOWN-CHANNEL EFFECTS

An additional element of redundancy, and the main defense against failures of interaction and trust, is the network of out-of-channel communications. Especially in a small bureaucracy like the Foreign Service, there is a great deal of communication other than directly up and down the line. All field officers, for example, check their understanding of the system's needs by comparing notes with each other. Some confusion, vagueness or

inconsistency can be detected by this cross-channel talk, and filters can be by-passed by working the desired information up another channel with more sympathetic superiors. Again, there tends to be a complex "sponsor-protégé" network--enabling a junior to pass information to a friendly figure at a higher level, or a senior to pass instructions to (or obtain information from) a lower level. Unfortunately, these networks, when overused, tend to erode the trust element of the basic system and cannot be as efficient. The promotion of professional trust and the de-emphasizing of out-of-channel communications are problems for the system managers, but the existence of multiple channels --through redundancy--makes the entire system more trustworthy and robust to the National Command Authorities.

VALUES AND DANGERS

The primary value of this system of channels is the accuracy and hard focus on important issues it provides by the concentration at each level on a body of issues small enough to be encompassed with successive and redundant filters ensuring relevance of transmitted information and, hopefully, storage of information which could become relevant. Moreover, with close contact, interaction and feedback, there is a high degree of confidence in the accuracy of the information which reaches the highest levels.

The Foreign Service has attempted to reinforce the trust and confidence of interactive feedback in defining scope-of-work by requiring, as a part of the annual efficiency reporting, that each officer with his rating superior sign a mutually agreed upon statement of objectives against which the individual's work will be judged. There are provisions for continuous amendment of

this statement, and it provides an opportunity for increasing trust, confidence, and clarity in the system. Against indifference, however, it has no defense. Too often these objectives are written ex post, or are written in such broad terms as to provide little or no true guidance.

The dangers of the system are primarily these: 1) the process of channelling and filtering consumes time, very often so much time that appropriate action is defined only after the time for such action is past; 2) the system, by promising accuracy, rewards caution, compromise, and lack of clarity. (Low-probability assessments--even if accurate--tend to be filtered out, and those estimates which are passed upwards have tacked on the qualifiers and caveats of each successive level until too often the facts are lost among the temporizations, and 3) a lack of reinforcement in the system for accurate interactive feedback, clarifying each level's scope-of-work in an atmosphere of trust and confidence, allows wide disparities between each level's perception of U. S. interests. This results in loss of efficiency, with effort consumed by irrelevant issues, so that often the information available does not match the needs of the policy makers.

TIME VS. ACCURACY TRADE-OFFS

At the present time, the U. S. Government tends to deal with foreign affairs in a crisis-prevention or crisis-reaction mode. Even in ordinary issues, the action level demands information immediately. The usual response is to trade accuracy for time. An intermediate level, unable to obtain the information from the field in the demanded time, answers on the basis of general knowledge or information supplied earlier, half-remembered and possibly seriously dated, thus cutting out of the system all lower levels. As the principal

value of the system lies in its concentration on a small body of issues at each level, when the level which responds does so outside its area of expertise, the accuracy value of its response will be limited, albeit timely.

ACCURACY VS. USEFULNESS TRADE-OFFS

Another serious problem has two aspects. Where there is any failure of communication down the line, the field officers will focus on, report on, and analyze issues of little or no relevance to the decision maker--highly accurate, but not useful. This is particularly true where events are changing issues rapidly. This problem relates to speed of communication. The system must not only transmit needs down and analyses up, but must be able to do so fast enough to react to sudden shifts, which is difficult (and may be, at times, impossible). A similar problem is caused by the ratio of demands to time and manpower. Whenever (usually) the requirements exceed available time, the responding level tends to focus on the questions easiest to answer, leaving the more difficult (and normally more important) questions for some later date which never comes. Thus the system becomes overloaded with highly accurate trivia, while proudly boasting of a 90% response rate. (In Iran, the monthly report of visa issuance, the local wage-rate survey, the analysis of Central Bank reserves, and the visitors' list were up-to-date until February 14, when the embassy was occupied for the first time.)

HOW SHOULD THE SYSTEM DETERMINE TRADE-OFFS

If the managers and members of the system were to understand and acknowledge that these are trade-offs, much of the dangers of such trade-offs would disappear. It is the myth that "everything can be accomplished" which causes problems. If an assistant secretary, desk officer, or ambassador responds to

an urgent demand with the statement that "The best answer available without checking with the knowledgeable source is . . .," the questioner has the option of proceeding carefully with less-than-perfect information, or of accepting a delay to get better information. It is when he acts believing that he has the best information that errors are made--and blame apportioned. If a new information request of minor value had to be approved on the basis of eliminating some other request, fewer such would be made.

Until the Foreign Service begins to examine and analyze itself and identifies the real trade-offs it must deal with, these problems will remain. While it publicly asserts that problems do not exist (and privately spends its energy covering up problems), it will be increasingly seen as incompetent. While the system is proficient at "single-loop learning," to use Chris Agyris's terminology, which involves changing responses to demands so as to avert criticism or requirements for basic change, it has not mastered the skills of "double-loop learning," that is, learning how to restructure functions and system basics to resolve problems the original system was not designed to meet.[5] If it is accepted that this system can provide accuracy (but not at speed), while U. S. interests now demand speed, the system must either change by giving up some accuracy for more speed, or find a new niche for itself in the organization where accuracy is still valued, while allowing some other part of the organization to provide the speedy responses demanded. For example, the Foreign Service might well determine that, if it is to properly fulfill its intelligence function, it must either significantly increase its personnel and budget (to reduce the demand-per-officer and allow for much faster communication between levels) or it must abandon extraneous functions which now absorb its officers' time. However, the State Department has, in the pro-

cess of "defending its turf," resisted strongly (albeit with little success) any encroachment of other agencies into our overseas posts, and insisted that Foreign Service Officers can and will handle commercial, drug, agricultural, and other areas. Even when other agencies win a place, the Foreign Service tries to duplicate that agency's efforts. For example, in each post where the Drug Enforcement Agency (DEA) has won a position, one political officer is assigned as embassy narcotics control officer, and told to oversee the work of the DEA agent. During this same period, the Foreign Service has accepted a series of personnel and position cuts overseas, plus a series of Congressional reporting demands rising from Congressional distrust of the service's competence, all the while maintaining its "can-do" attitude. To resolve these problems the system must admit to their existence, determine the real trade-offs involved, and either amend its functional structure or modify its goal structure until it is able to satisfy the demands placed on it.

CENTRALIZATION--CUTTING THROUGH THE BARRIERS

There are times when the trade-offs implicit in the system of channels are unacceptable, even when recognized. True crisis events demand response, on the basis of the best information available, even if not as accurate as possible. Failing an alternative, the decision maker can only act, and pray that he does not make too serious an error. A modern C^3I system of direct centralized communication is an alternative, however, and is currently available to some extent. During the Cuban Missile Crisis, President Kennedy wished to talk to his ambassadors in Moscow, London, and Mexico during those hours when Russian ships carrying missiles approached Cuba. Not only was the White House operator unable to reach them, it was found that State Department telegrams

to each post instructing the ambassador to call Washington would not be received until each post opened for duty. Following the crisis, the State Department was instructed to develop and establish a 24-hour worldwide communications center, and an automatic telegraphic priority system, which would enable it to maintain direct communication to every Foreign Service post at all times. The resulting State Department system, operating out of the Secretariat Staff/Operations Center is a fully integrated command post with multiple communications systems, automatic priority on commercial circuits, interconnectivity into the military and White House communication nets worldwide. The staff constantly updates both residential and official contact numbers with direct lines to the department principals' homes, able in most cases to establish voice-grade communications between any two points within minutes, and capable of establishing secure voice/data/(and sometimes) visual secure circuits with most important posts.[6] This is the center from which diplomatic crises and special projects (e.g., the Iranian hostage situation) are managed, utilizing special task forces drawn from all levels working directly with the Secretary or other senior officials. During the first takeover of Embassy Tehran (February 14-16), the embassy was in secure voice contact with the operations center until the embassy equipment was destroyed (as the invaders reached the secure vault). After some difficulty, it re-established communication with the ambassador through a U. S. military airborne communications platform to Consulate Isfahan, to landline to an apartment in Tehran, and to walkie-talkie to the ambassador, who was able to consult with the Secretary before surrendering. Using this system, the National Command Authority, or a lower level decision maker, is normally able to consult directly with the field officers most directly knowledgeable about a problem area in real time, and then to act on that information.

Unfortunately, this system is far from perfect. A major problem may be the training of the participants. Analysts accustomed to carefully concentrating on and examining their statements before transmitting a telegram might say very different things when asked in a hurry over a telephone line. Moreover, there is no guarantee that the decision maker knows the right questions to ask. Being normally quite separate on the chain of "normal channels" the pair speaking do not have the shared background and understanding characteristic of adjoining links on the usual system, and unless they are aware of this lack, they may be speaking at cross purposes. Even if they are aware, they may spend their time on unnecessary background. The embassy in Tehran spent over a half-hour trying to explain to the Secretary just who it was attacking the embassy. The task force members often have to spend a considerable time developing a common language before they can work effectively together. On a broader scale, many past crises have shown that the crisis atmosphere encourages the immediate and the expedient over the best or even better actions. Records are often poorly kept, and tired people make mistakes which must eventually be rectified. Moreover, the existence of the system--with its psychological rewards of immediacy, high-level collaboration, and excitement--encourages its use.

In the Department of State, success (or at least relative importance) for an individual, office, or issue-group is largely measured by access to, and the attention paid by, the Department's principal officers. Since the Secretary must personally authorize the formation of an Ops Center Task Force, the elevation of a crisis to Ops Center proportions explicitly guarantees both access and attention. Thus, crisis management shares with classification and special handling indicators the danger of excessive escalation. Something

may be top secret, or NIACT (night action) NODIS (no distribution outside Department of State), or a crisis not because it warrants that treatment, but because that treatment increases the chances of attention or "success." Finally, its successes permit the belief that it will always be successful, while its failures tend to be subsumed in the basic diplomatic problem.

VALUES AND DANGERS

The direct communications and control system allows immediate access to the best available information in a situation where action is demanded and accuracy must be traded off for time. It allows immediate reaction to fast-changing situations, and at its best can involve every major link in the normal chain of information flow. Normally, however, it eliminates most or all of those links, allowing for misunderstanding because of the lack of shared knowledge between the participants. It sacrifices redundancy for immediacy, both in terms of multiple contribution of ideas, and often in terms of communications itself. While the system has physical redundance in terms of communications systems, its goal is a single fixed link which, if it fails, may be difficult to re-establish. (In the Tehran situation, the military airborne platform initially refused to establish the link with Consulate Isfahan because the crew members didn't know what a consulate was, and the consulate didn't possess the current password.) Moreover, the system is extremely expensive in comparison with usual methods, and is very difficult to cut off once it is begun. Task forces normally continue in the Operations Center long after any immediate crisis point is passed, when the usual channels could more efficiently, effectively, and accurately handle the matter.

HOW SHOULD THE SYSTEM DETERMINE TRADE-OFFS

A centralized system is both necessary and desirable during a crisis, but should be used with the clear understanding that its use entails a trade-off of accuracy and cost for time. This system should, when used, make every effort to involve every chain-element of the normal channels to ensure maximum information value in the communications. (By disrupting the normal flow of work, this should also encourage the early end of the crisis system when it is no longer necessary.)

INTERACTION BETWEEN CENTRALIZATION AND CHANNELLING

Ideally, perhaps, the elements of the centralized system should be fully integrated into the channelled system. Many of the benefits of the centralized system derive from advanced communications technology--the equipment which allows instant, real-time, secure communications directly between the decision maker and the one or several points of involvement with a particular crisis. If, as costs decline, these facilities were available routinely between all levels of the system, the improved speed and ease of interaction could resolve many questions and problems before they became crises. The centralization requirement for crisis reaction could be managed through a "communications traffic-controller" ensuring that any action level has priority access to whatever other levels, up or down, are necessary for decision making--thus obviating the need for most special task forces.

The availability of easy, real-time communications at each link of the chain should eliminate many of the time problems of the traditional system, while the familiarity of the channel members with the direct communication system would sharply increase the accuracy of information passed in crises.

However, there would always be sharper crises which could not afford the time of involving the traditional chain; so two systems would always exist, and the present cost of the technology rules out a total integration in the near future. In that case, we must consider carefully what situations call for the appropriate use of which system.

A RECOMMENDED APPROACH TO TRADE-OFFS

In those situations involving large quantities of complex information, where a wide range of options are available and there exist a wide range of possible results, the system which provides the greatest accuracy is essential. In those cases, a trade-off with time is unacceptable. If time is also of the essence, the trade-off should be between time and money. Let sufficient funds be expended to improve communications for the traditional system such that its highly accurate analyses are available without unnecessary delays. The traditional system can also be improved by increasing the prioritization of the demands on it. As situations require careful analysis and accurate information on a single or few issues, let other requirements on the system be dropped to increase focus. In situations where action is essential, careful consideration should be given as to the appropriate decision level. Where possible, the decisions should be made at as low a level as has the trust of the authorities to bring the maximum amount of pertinent background information to bear, but once this is done, a crisis communication system should be fully utilized to minimize time spent before decisions.

COMPETITION AND CROSS-FERTILIZATION

At the present time, it is both necessary and useful to have the two systems existing together and competing with each other. The danger arises

that the defects and relative strengths of each system will be seen only through serious errors or disastrous effects from using one or the other in a given situation, but it is certainly possible that instead each system will be allowed to borrow from the other until both are strengthened.

A problem occurs when each system's borrowing reinforces weaknesses--rather than strengths. The task forces set up to handle emergencies increasingly are becoming institutionalized with a growing membership, growing complexity, and a decreasing ability to respond immediately to emergency demands, while (lacking the necessary structure) they do not become proportionally more accurate. (The Iran Task Force, established February 14, 1979, to respond to the first attack on Embassy Tehran, is still in 24-hour operation in the Ops Center with a full time staff of 43 as of April 1980.) The normal bureaucratic channels, at the same time in competing for attention, are becoming characterized by "crisis-management" patterns with great emphasis on speed of reaction and less time for thoughtful analysis and a lower level of accuracy. Great attention is necessary to ensure that action patterns arise from functional capabilities, rather than unthinking imitation of the apparent virtues of another system.

In the ultimate crisis, a nuclear war, a centralized C^3I system will be essential if U. S. society is to survive. It is highly likely, however, that it will have to be a C^3 system without any current intelligence. On the other hand, if a traditional intelligence system is strengthened with some of the technology of C^3I, we may defuse crises early enough to avert that war.

STRUCTURING THE SYSTEM (RESTRAINTS AND SUPPORTS)

Before we can develop the intelligence component of an integrated C^3I system, we must modernize, improve, and make better use of our current

intelligence system. When the Iranian Crisis results in a cry from the White House of a "failure in intelligence," it is clear that the National Command Authorities are far from understanding the requirements of an accurate, timely system. The first step must be in developing an awareness at the highest levels that no system can respond to their needs until and unless they work to transmit an understanding of those needs to the system, and through the levels of the system. A great deal of minor work can be done to improve the accuracy and relevance of intelligence reporting, but the major barrier now is psychological. When rigorous analysis is rewarded more than errors of judgment are blamed, the system will be moving toward improvement. Much can be done to improve the timeliness of the system, but until evidence of professional trust is rewarded more than bureaucratic infighting, the usefulness of the material is not likely to change. A simple, but expensive, element of necessary restructuring is an equation of requirements with manpower. If requirements are decreased, or manpower increased, the essential strength of the existing system--competent officers concentrating on few enough issues to comprehend--will be strengthened. If the trend of the past decade continues--constantly increasing requirements on a declining workforce--the information derived from the system will be of decreasing value. Perhaps it is time to pause in the hardware phase of C^3I development, and to concentrate instead on the examination of the needs, duties, and capabilities of the human elements on both the command end and the intelligence end.

NOTES

1. Miller, James Grier, Living Systems (New York: McGraw Hill Book Company, 1978), Ch. 3, "Structure and Process," pp. 51-65.

2. Chapman, J. and McGhie, A., "A Comparative Study of Disordered Attention in Schizophrenia," Journal of Mental Science, 1962, 108, pp. 487-500.

3. Miller, J. G., op. cit., p. 169.

4. Forrester, Jay W., "Counterintuitive Behavior of Social Systems," Technology Review, v. 73, no. 3. Jan. 1971, pp. 1-16.

5. Argyris, C. and Schön, D. A. Organizational Learning: A Theory of Action Perspective, Addison-Wesley, Reading, MA., 1978.

6. U.S. Department of State, The History of the Ops Center, 1968 (unpublished briefing material).

BIBLIOGRAPHY

Bleakley, J. "The Future of the Foreign Service." Foreign Service Journal, November, 1979, p. 12.

Chapman, J. and McGhie, A., "A Comparative Study of Disordered Attention in Schizophrenia." Journal of Mental Science, 1962, 108, pp. 487-500.

Clark, J. M. "Improving Substantive Reporting and Analysis in the Department of State: Recommendations," 1979 (unpublished memorandum).

Department of State, "Automation in the Department of State in the 80's." Information Systems Office (O/ISO), March, 1979 (draft report).

Emery, F. E., ed. Systems Thinking. Middlesex, England: Penguin Books, Ltd., 1972.

Forrester, Jay W. "Counterintuitive Behavior of Social Systems." Technology Review, v. 72, no. 3, Jan. 1971, pp. 1-16.

Forrester, Jay W. Principles of Systems. Cambridge: Wright-Allen Press (second edition), 1976.

Miller, J. G., op. cit., p. 169.

Miller, James Grier, Living Systems (New York: McGraw Hill Book Company, 1978), Ch. 3, "Structure and Process," pp. 51-65.

6. THE SOVIET DOCTRINE OF TROOP CONTROL --A PRIMER

Marc Dean Millot

TABLE OF CONTENTS

INTRODUCTION

This work is meant to serve as a primer on Soviet doctrine of troop control. In military affairs doctrine can be defined as prescribing the methods of use of equipment to meet the objective of engagement in battle. Thus there exists a strong linkage between technological possibility and the desired goals of military action. Doctrine, which serves as a guide to action in the application of weapons systems to military requirements can then also serve as a predictor of action of some extent.

That doctrinal thinking has preceded actual weapons deployments and force structure changes in the Soviet military is shown in several cases. Soviet doctrine of the offensive developed in part by Marshal Sokolovskii, requiring large numbers of tanks, armored personnel carriers, massive airpower and particularly tactical nuclear weapons preceded the development of such forces. Likewise, Admiral Gorshkov wrote of the long-term strategy of the Soviet Naval Forces and the necessary equipment to carry that strategy out long before the deployment of comparable ocean-going weapons systems--and even today the Soviet fleet has some ways to go before it equals the tasks set for it in Gorshkov's latest work, The Seapower of the State.

Because doctrine has proven to be of some predictive value in Soviet land and naval practices in these cases, there is reason to believe that it may hold true for the doctrine of troop control as well. If this is so, then it would be of some importance to understand how the Soviets view problems of command and control in a military environment. How do they think the new "electronic" revolution has affected war fighting? What are the goals of their troop control system and what problems do they see blocking perfection?

What are the fundamentals of their conception of military cybernetics? What principles and methods are the basis of their current doctrine of troop control? How is their system of troop control organized, what are its constituent elements, and how do they interrelate? What do they see for the future of control systems and their increased automation?

This primer attempts to survey these questions and their answers in the words of Soviet military theorists. First, because they say what they mean better than I could recount it. But second, because it is important to catch the subtle distinctions in their analysis that a review would miss. My explanatory notes and summaries are primarily meant to tie together the various sources and maintain a common thread of thought.

The authors of the excerpts used in this paper are among the luminaries of Soviet military doctrine. General Sokolovskii and Admiral Gorshkov are the fathers of modern Soviet land and naval doctrine. The other authors are prominent in the "Soviet Military Thought" series, a collection of Soviet military writings--including texts used in the training and indoctrination of officers--"must reads" for the rising young stars of the officer corps, and anthologies of works from the Soviet military publications such as Red Star.

The authors of these works are generally part of the Soviet military training/education institutions. They are often retired officers now serving as professors but younger students have been known to contribute as well. Col. V. M. Bondarenko (ret) is a frequent contributor to Communist of the Armed Forces (a Soviet military publication), a professor at one of the Soviet military universities, and an expert in control doctrine. Gen. Col. V. V. Druzhinin and Col. Engineer D. S. Kontorov, authors of Concept, Algorithm, Decision, also possess respected experiences. Druzhinin, who holds a Phd. in

Military Science, was Deputy Commander-in-Chief of Soviet Air Defense Forces (P.V.O. Strany) and served as Deputy Chief of the General Staff of the Soviet Armed Forces after 1970. Kontorov is a Doctor of Technical Sciences. The "Forward" to Concept was written by General of the Army S. M. Shtemenko who is First Deputy Commander-in-Chief of the Joint Armed Forces of the Warsaw Pact Nations.

The co-authors of The Revolution in Military Affairs, an anthology of articles published in Moscow in 1973, are "recognized as spokesmen of Soviet military affairs" as the American editors' commentary notes. Col. N. A. Lomov, the book's editor, was assigned to teach at the General Staff Academy, an institution similar to the American Armed Forces National War College. The other contributors are not as widely known, but the book and Concept, Algorithm, Decision are part of the Officers' Library Series, a 17-volume collection designed to bring officers the latest in the Communist parties' accepted doctrine.

Joseph D. Douglass Jr., author of The Soviet Theatre Nuclear Offensive, is one (of only two non-Soviet authors) who has studied the troop control doctrine of the Soviet Union and published work in an open and available fashion. I included part of his analysis and adopted a strategy similar to his own of relying primarily on the Soviet authors themselves to explain their doctrine, rather than paraphrasing their work and then missing some of their intentions.

The other non-Soviet author I used in my research is Charles S. Sheldon II, the Congressional Research Service's expert on the Soviet space program. He is also one of the few people to publish anything to do with Soviet hardware related to troop control. After consulting his work to determine if I

could compare doctrine to deployments in any meaningful way, I decided that I could not. Sheldon himself relies on mirror-imaging American practices onto Soviet equipment because the Soviets do not designate any satellites they send up as civilian or military. Although our military knows, that type of information tends to be classified.

This paper is divided into six subject areas:

- The Revolution in Military Affairs;
- Problems and Goals of Troop Control;
- Soviet Military Cybernetics and Man-Machine Theory;
- The System of Troop Control;
- The Process of Automation.

A short commentary to tie these areas together serves as a Conclusion.

AN INTRODUCTION TO SOVIET TROOP CONTROL DOCTRINE--THE REVOLUTION IN MILITARY AFFAIRS

Soviet military doctrine recognizes the profound change in conduct of warfare brought about by new technologies since the introduction of the atomic bomb. This scientific progress has resulted in a "revolution in military affairs," and demands new styles of war/fighting and organization.

> The scientific technical revolution has determined the prospects for the development of modern military affairs, and has posed a large number of problems, the solution of which has raised Soviet military science to a new, higher level. The complexity of modern military affairs is generally recognized, the process of its improvement is continuing, and it would be hard to name any area which did not depend on the overall development of production, science and technology.[1]
>
> The destructive force and range of nuclear weapons and the speed of military operations comprise that 'minimum' of the basic qualitative features which characterize the new patterns of modern war.[2]
>
> Nuclear weapons are characterized by a great destructive and devastating result as a consequence of the effect of an entire complex of destructive factors including the shock wave, radiant energy, penetrating radiation, and fallout. The use of these weapons has fundamentally altered the nature of combat, the operation, and the entire war as a whole.[3]
>
> Historical experience shows that as productive forces (particularly industrial production), science, and technology increase, there is also a steady development of weapons and military equipment in general, which plays an increased role in warfare. Moreover, the development of weapons inevitably produces changes in the method of conducting military operations as well.[4]
>
> The distinguishing feature of weapon development under current conditions is the appearance of qualitatively new types of weapons and military equipment and their rapid and massive introduction into the armed forces. This has led to a pronounced improvement in the latter's combat capabilities, a radical break in the organizational forms of armed forces and methods of conducting military operations on every scale. Military strategy and the art of war as a whole

have undergone a revolution.[5]

> Now, in addition to nuclear weapons and missiles, still another new and very important military technical factor has emerged which undoubtedly will exert a marked influence on the nature of war. We refer to the use of electronic gear, in particular, electronic computers and various other types of equipment, by the armed forces, and other devices for automatizing and mechanizing control and command over weapons and troops as a whole.[6]

> The development and introduction of missiles, nuclear weapons, and electronic equipment have led to fundamental changes in almost all other weapons. As a result, the relative importance and strategic purpose of the various branches of the armed forces and their military employment have so changed that a wholly new nature is foreordained.[7]

Scientific-technical progress since World War II has led to a revolution in military affairs, according to Soviet doctrine. This revolution is the result of the introduction of atomic weapons, missiles, and the electronic equipment that guides and controls delivery and detonation of the missile and weapon to the targeted objective.

Prior to the introduction of these weapons, military operations primarily took place "in ground theatres, where the results, in the last analysis determined the outcome of the entire war . . . The available means of destruction [conventional explosives, tanks, airplanes, artillery and infantry] did not make it possible to achieve a rapid change in the relationship of forces between sides; therefore military operations developed relatively slowly."[8] War was a relatively static and drawn out affair when compared with possible alternate scenarios of war that might be inferred from the capabilities of the new weaponry.

To the Soviet military the introduction of the new weaponry changed the nature and speed of warfare. First, warfare is no longer static; the missile can leapfrog static defenses opening up the rear lines of defense and logistics

to attack. Second, the speed of missiles and the massive destructive ability of atomic weapons make the rapid conclusion of hostilities with the decisive victory of one power more possible.

Without precise and reliable means of missile guidance and weapon detonation, however, the ability of the weaponry to achieve military objectives rapidly would be severely diminished. Electronic devices allow reliability and precision.

The offensive punch of nuclear missiles, with their electronic guidance and detonation systems, create a wholly new defensive environment. Troops, their weapons, and the logistical support structure must be hardened against the effects of nuclear explosions.

The operational requirements of both defensive and offensive modes of warfighting are such that rapid effective, redundant means of communication between the military decision makers and the users of weaponry are absolutely vital. In the revolution in military affairs "troop control" gains a central importance.

> Under present-day conditions, combat can be carried out on a global scale, and in all spheres (on land, in the air, and at sea) with the possibility of an active effect from one sphere on another. In battle enormous masses of men will participate on both sides, and these men will be controlled from single centers through a complex and diverse structure of control bodies.[9]

Problems and Goals of Troop Control

Soviet military theory defines troop control as follows:

> By control in the broadest sense one has come to understand the purposeful effect of the control body on the controlled object.
> The essence of troop control consists in providing constant purposeful leadership by the command and staffs over all the activities of the subordinate troops.[10]

> In each system of troop control, there is the controlling body (the commander, the staff, or command post), the object of control (the troops with their weapons, the combat complexes, and so forth), as well as the communications channels between them over which one receives reports while the other receives signals, commands, and orders.[11]

> Combat means and their rapid action were to a certain degree commensurate with the possibilities of man. Control of the forces was achieved by means of previously evolved methods familiar to all, without the use of complex machines and equipment. Only three decades have elapsed and the former approach is largely outdated. The immense power of the means of strike, increase in their length of range, the scope of combat operations and the growth of rapid operation of the means of combat to such a degree that it is already incommensurate with the physical possibilities of man, are forcing one to take a fresh look at the most important aspects of waging struggle . . .[12]

> The volume of information that staffs must process has increased manyfold since World War II, and the time allowed for decision making has decreased manyfold. As a result, the brain capacity of commanders and staffs have increased vastly. To meet these requirements by simply expanding the administrative apparatus is fundamentally impossible, since this could require an inordinate increase in the number at headquarters. Organization of efficient operation within such vast management offices would become a very difficult task.
>
> The only escape from this incompatible situation lies in the extensive application of automation, primarily computers.[13]

> It has been calculated that, during combat action where nuclear missiles are used, the headquarters of a division will receive more than three times as much information as the headquarters of equally large formation received during World War II.[14]

The "global reach" of the superpowers and the increased use of combined operations (air, land, sea) in the dangerous nuclear environment have changed the nature of troop control. Prior to the revolution in military affairs a commander could generally be within each reach of his weaponry due to his physical proximity. The massive number and types of weaponry used today when combined with military operations that may span the globe do not allow the commander easy access to his troops.

The demands on the commander have increased; he must control more troops and weaponry over a larger area with shorter time to make decisions. Proper decision-making is even more important than in the past, because the rapid means of nuclear attack allow the enemy to easily exploit the commander's errors of judgment and deal a decisive blow.

More information, shorter decision times, and wider areas of operation and heavier prices paid for errors of judgment overwhelm the mental capacities of man.

> The possibilities for carrying out mental types of labor (and troop control is precisely such a type) are limited by the range of the sensitivity of human organs of perception, by the capacity of his memory, by the reaction time, by the speed of the thought process, and by the quantity and quality of knowledge acquired as a result of training and expertise in life.
>
> As for broadening the possibilities of man to perform mental types of labor, here scientific-technical progress in this area has begun to be markedly apparent only in recent years.[15]

Computers are man's answer to the less time/more data problem. They can rapidly assimilate, collate, and categorize information. They can quickly make calculations that humans might take days to accomplish. Computers help resolve three contradictions the environment of modern warfare presents:

> 1) "Proficiency" vs. "high level of control." Decisions must be made quickly and in a nuclear exchange situation almost instantaneously but these decisions must be made without error.
>
> 2) The expanded scope of commander responsibility across wide geographic areas increases the possibility that "particular elements of the control system will fail" but it is vital that hight reliability be the systems norm.
>
> 3) The big picture necessitates centralized and close control over subordinate units but local officers need the ability to take their own initiative.[16]

The Soviet military calls it the "problem of the century:" how to achieve the ". . . complete utilization of the experience and intellect of man and integral combining of it with the speed of the computer."[17]

Soviet Military Cybernetics and Man-Machine Theory

To the Soviets, military cybernetics is:

> . . . the problem of automation of processes related to the development of the required data for decision making . . . is . . . the basis of military management.[18]
>
> . . . commanders and their staffs require a thorough understanding of the methodology, scientific tools and techniques of decision making.[19]

A close knowledge of the automated systems workings is a new requirement for proper commandership.

> Automation systems are components of a weapons system. They should be efficient, reliable, and easy to use. Like any weapon, they must be mastered completely. It is essential to know the system and the principles of military application, to become accustomed to them and, if you desire, to love them.[20]

How exactly to integrate the concepts and hardware of military cybernetics is a problem recognized by the Soviet theorists, as the following mock discussion points out.

> In spite of the fact that the world literature abounds with publications on automation and new achievements in cybernetics, delay is perceived in the development of the ideological aspects of the problem. The trend toward 'total' automation of management, which saturates scientific-technical propaganda, is not always wholeheartedly supported, and sometimes considerable skepticism is expressed. The 'automaters' and 'intellectualists' have been engaged for a long time in a discussion that goes something as follows:
>
> The former: 'Here you have the cybernetic industry and its capabilities, so use it. If the capabilities are inadequate tell us what you need and we will do it.'
>
> The latter: 'We are ready and want very much to use cybernetics and you are welcome to expand its capabilities. We place great value on the computer. But tell us how it will help us to solve management problems and prove that it has the advantages which you say it has. Otherwise it will be hard for us to understand how to use it.'
>
> The former: 'Such statement of the problem is unacceptable. This is not our field. Take the computers and learn how to use them; then the advantages will become obvious. Otherwise let us know what other equipment you need for your problems.'

> The latter: 'To produce a positive effect the equipment must possess certain properties. Apparently you don't know very well what these properties are, because you ask us what we need. But in order to answer this question we must know what you can do and particularly for what purpose.
>
> The discussion returns to the starting point.
>
> Everyone agrees that automation should heighten and ennoble man's labor; most people are in favor of delegating some of their functions to automate, but no one can yet determine the limits of their capabilities and benefits. This is the essence of the problem.[21]

The problem of contradiction arises between human creativity and ability of a computer to rapidly calculate. The Soviets admit that humans fear that their creative abilities will be superseded by the computers seeming infallibility. How does this contradiction get resolved?

> It is very tempting to assume that the truth lies somewhat in between: man does a little, the computer does a little, there is some intuition, a bit of arithmetic, and then, on the basis of the actual breakdown of the situation it is possible to divide the spheres of influence of man and machine and thereby answer the question, at least for the near future. In military science such a compromise position is considered unjustified and incorrect.[22]

> Marxism-Leninism teaches us that the truth lies not in conciliation, but rather in the dialectic unity of contradictions. In the case at hand we are speaking of combining the capabilities to stimulate dialectic development . . . sober calculation and creative fantasy . . .[23]

> Automation does not replace and does not supplant creativity. Automation carries to a higher, more general level.[24]

> The technical control devices which have been created and are being created due to scientific-technical progress, in turn themselves become one of the driving forces of this progress. They serve as the material base for automating and mechanizing the control process.[25]

> At the outset we will assume that the 'man-machine' system is more perfect than 'man' or 'machine' alone.[26]

> In order to achieve effective interaction between man and computer it is necessary that man do the thinking and the computer do the computing.[27]

> Man thinks faster than he formulates a result, and exchange of information at the level of intermediate ideas and judgements is important for joint operations. It may seem paradoxical, but the information capacity of human-machine interaction (and consequently group-machine interaction) will increase faster than that of man-man interaction, and in a short time the technical means of interaction will leave the natural communication modes (especially speech) far behind. When this happens, computers, equipped with corresponding accessories, will become an effective means of interaction between people.[28]

Principles and Methods of Troop Control

As noted earlier the Soviets define troop control as follows:

> By control in the broadest sense, one has come to understand the purposeful effect of the control body on the controlled object.
>
> The essence of troop control consists in providing constant purposeful leadership by the command and staffs over all the activities of the subordinate troops.[29]

Two problems present themselves to Soviet military theoreticians in their attempts to devise a working theory of troop control. The first relates to organizing combat, gathering information, making decisions, communicating those decisions to the troops, and then carrying out these decisions in combat. The second refers to measures necessary to support combat including political and morale preparation, rear support, leadership training, and organization of the services. Gen. Lomov notes:

> The [second] group of problems does not determine the essence of the control process, but without fulfilling it, the functions of organizing control would be limited and incomplete.[30]

The central problem then is the former: the gathering of information, analysis of the situation, and consideration of alternate solutions to the military problems, the making of decisions by the leadership, communication of decisions to the troops, and the following of those decisions by subordinate troops in a timely manner.

Before decisions can be made information must be gathered and analyzed.

> The basic demand relating to the work of acquiring situation data is the promptness, continuity, and reliability of the data.[31]

> For achieving the greatest completeness, accuracy, and reliability of the received information, it is essential to work for the coordinated use of all sources of receiving information. Here the most important information, as a rule, should be reported to the commander and also transmitted to the superior and subordinate staffs.[32]

Communications systems must be set up and tested well before war breaks out if the control system is to work.

> The preparation of communications not only includes securing the control of the Armed Forces when war breaks out, but also control of the country as a whole, and particularly of its economy.
>
> To do this, one must create in peacetime reliable control points capable of operating normally during an enemy attack with weapons of mass destruction and capable of ensuring reliable communication between these control points.
>
> The creation of reliable control points involves their proper locations and equipment and the preparation of duplicate facilities provided with modern communication equipment.[33]

> Peacetime and wartime communications must be developed on the principle of systemic continuity.[34]

> Multichannel radio, radio relay, and underground cable lines should be a basic means of communication in preparing for an enemy nuclear attack. Above ground communication lines passing through major population centers and can centers must include underground cable bypasses at these points and alternate communication centers.[35]

> Important communication centers should be constructed underground and protected from nuclear explosions. These centers should be distributed in a communications network which will allow by-passing in case any of the centers are put out of commission. It is very important to create reserve mobile radio centers to support needed areas.[36]

Modern warfare is fast paced; correct decisions must be made and carried out quickly. The Soviets demand that control be proficient; commanders

should:

> spend as little as possible time on the control process in order that the maximum possible time is available to the troops.[37]

And they demand that a high level of control be maintained; commanders must "take and carry out the best decisions."[38]

Soviet analysts recognize that there is a possible contradiction between quick decisions and correct decisions. They hope to resolve this contradiction through:

> the use of the most rational methods of control as well as broad application of the most recent technical devices . . .[39]

The rational methods of control include rigid adherence to the following principles of troop control:

> Sole responsibility. The principle of sole responsibility in terms of control must be understood as concentrating the rights of leadership over subordinate troops in the hands of one commander. These rights are given him by state laws which determine the basic principles for development of the armed forces and are regulated by the regulations and orders of superior chiefs.[40]
>
> Sole responsibility in the Soviet Army is based upon the high political awareness of each superior who in his activities follows the decisions of the CPSU, as well as upon the monolithic political and moral unity of all personnel. The principle of sole responsibility presupposes not only the sole taking of decisions by the commander, but also his complete personal responsibility for the taken decision, for controlling subordinate troops, and for successful execution of their missions.[41]
>
> Collectivism. Under modern conditions, due to the significant increase in the range of tasks related to troop control, the complexity of the entire control process and the sharp rise in responsibility, particularly for using nuclear weapons, it is beyond the capacity of a single person to control troops in combat, let alone major operations on a strategic scale. For this reason the principle of collectivism in control is assuming ever greater significance. This is manifested in the fact that

the settling of the most important and crucial questions, particularly in the tactical and strategic elements, is done not by a single person but rather a group of responsible persons. Moreover, in the process of working out the decision, as in the process of troop control as a whole, the commander receives great help from his staff. However, the principle of collectivism in decision taking is not contradictory to the principle of sole responsibility. The taking of the final decision as well as the right of sole leadership and responsibility remain for the commander.[42]

Centralism. The superior level must unify the efforts of all subordinate forces and means, and coordinate and direct their actions for achieving the overall goal of the battle. Here only the senior commander is given the right to alter the methods and directions of the subordinates' actions in the course of their execution of the mission.[43]

Rigid centralization is particularly advisable on the question of using nuclear weapons and other powerful means of destruction, since here their most effective and efficient use is achieved. Moreover, centralization in the use of these means makes it possible to better coordinate the actions of all the forces and means on the spot and in terms of time. . .[44]

Independence and initiative. The increased fire and strike power of units and formations, and consequently, their independence in carrying out the set missions, the wide use of operations along axes, and the great dynamism and unevenness in the development of combat and the operation require a closer combination of centralized control with the providing of greater independence to subordinates and the manifesting of greater initiative and creativity by them in choosing the methods of actions. This is all the more essential due to the fact that in line with the rapid and frequent change in the situation, a prompt response to a change in it by the senior chiefs becomes more and more difficult.[45]

The encouraging of independence and initiative is also advisable due to the fact that excessive supervision of subordinates, as a rule, develops passivity in their actions and, equally dangerous, undermines their confidence in themselves. Moreover, with such a situation, any basis is lost to demand complete responsibility from them for carrying out the mission.[46]

Ability to foresee. An ability to foresee changes in the situation and the probable course of combat is inherent only to a person who possesses a dialectical method of thinking . . .

. . . the ability to foresee is inherent only to a well-rounded and experienced officer who possesses a broad strategic and tactical viewpoint.[47]

Constant knowledge of the situation. . . . foresight is based primarily upon constraint knowledge of the situation.

Profound and complete knowledge of the situation is the sacred duty of the commander and his staff, and for this reason is one of the most important principles of troop control.[48]

Firmness of control. Taking a bold decision and carrying it out steadfastly.[49]

Flexibility of control. . . . in working constantly to carry out the taken decision, the commander at the same time should respond to all changes in the situation, consider them and in accord with this adjust the decision on missions for the troops, and if need be, fundamentally alter the plan of combat or the operation.[50]

Continuity of control. . . . constant leadership by the commander over the actions of his subordinates and his influence on the course of combat.[51]

. . . the necessity of observing the principle of continuity of control places increased demands upon the subordinates as well. First of all they must show constant concern for maintaining contact with superior chief, and 'seek contact' with him; if for some reason it should be lost. Moreover, each commander should be constantly up on the overall situation, and know and thoroughly understand the overall intention of the superior chief. This will not only give him the opportunity to show reasonable initiative within the overall intention, but will also make it possible in the event that the command post of the superior level is knocked out to assume leadership of all the troops and carry out the overall mission.[52]

Concealment of plans. The arming of the opposing sides with such powerful means of destruction as nuclear weapons makes the possibility of thwarting the enemies intentions completely realistic. For this purpose, each of the sides will endeavor by all ways and means to discover the essence of the enemy's maneuver. In this regard, in modern combat and operations, the role of surprise in actions rose significantly. Surprise can be achieved only by the strictest concealment of the measures being prepared . . .[53]

High proficiency. Prompt response to all changes in the situation, that is, the prompt taking of decisions and the assigning of missions to the troops.

. . . high proficiency in work has nothing to do with hurrying.[54]

The above principles are intended as general guides for commanders and their subordinates. They are not rigidly prioritized laws, but flexible

guidelines for action adaptable to the entire variety of warfare situations. The overriding aim is the objective of the battle, as the principle of continuity of control suggests, and all control ought to further that end. At most times this calls for rigid centralization of control, but the independence and initiative allows the local commander latitude in the carrying out of his assigned tasks proportionate to the inability of his superiors to precisely direct his forces.

Although a number of contradictions between principles are recognized by Soviet doctrine--for example, between firmness and flexibility, or independence and initiative and centralization--Soviet control thought creates the union of opposites. There is a clear example of the use of dialectic reasoning in Soviet military doctrine. The thesis--"creativity" and antithesis--"organization" combines to form the synthesis--a Soviet troop doctrine of troop control, which through the historical material improvement of electronics, is capable of meeting the necessities of both speed and accuracy in every phase of the control process.

> As we can see, the significance of observing the above-indicated basic principles in troop control has greatly increased under modern conditions. At the same time, their observance requires creativity and precise organization in the work of the commander and his subordinate control bodies considering the new conditions for conducting combat and the specifically existing situation.
>
> These high demands, in turn, necessitate further improvement in the organizational structure of the control bodies, the equipping of them with more advanced technical devices, as well as an improvement in the work methods of commanders and staffs.[55]

The System of Troop Control

As stated above, to the Soviets the essence of troop control is the relations between the coordinating and subordinate units. Thus, three areas of

importance suggest themselves: the commander and his responsibilities, the subordinate units and their ability to obtain the objectives of battle, and the electronic equipment that ties the two together in intelligence gathering and analysis, and communications.

The commander. Many of the requirements of a good commander have only indirect relation to the specifics of troop control. Political training, the ability to keep morale high, courage and boldness all play a role in increasing the ability to control troops. But as stated in the last section, although these are important, they do not constitute the essence of control. Soviet writings on military psychology and leadership would be better sources on this subject than those on troop control. It must be noted, however, that as in any army, leadership skills are a part of the control process of the Soviet military.

The commanding officer is the most central part of the control system.

> The activities of a leader are comprised of two inseparably interrelated aspects. The first is the preparing of people to carry out definite tasks, as well as their daily training and indoctrination. The second is the control of people and the uniting of efforts of the entire collective on carrying out the set task. Decision-taking by the leader is the basis of these activities. The elaboration and taking of a decision on the basis of which the activities of both the leader as well as the entire collective are carried out is the most important element of leadership.
>
> The quality and level of leadership are determined by the end results of the practical activities of the led collective. Practice is not only the criterion of the truthfulness and correctness of various views or theoretical concepts but also an indicator of the leadership level. For this reason, the nature of leadership can be judged only from the results achieved in the process of practical activities.
>
> However in and of itself the success of practical activities still does not provide a right to judge the degree of leadership qualifications. Here it is also essential to establish at what price the success was achieved. The party condemns those leaders who endeavor to fulfill a plan at any

> price. The same thing is true in combat and military activities. The achieving of victory in one or another combat still does not describe the leadership level. There is the well-known expression "Pyrrhic victory," that is, a victory which is achieved at the price of unjustified losses. Such a victory does not show a high level of military leadership or its scientificness.
>
> Scientific leadership should provide the fullest utilization of the existing capabilities, and an achieving of maximum results from the practical activities with the least expenditure of forces and means. V. I. Lenin pointed out that in the leadership of social processes it is essential to work for 'a conscious choice of the means, procedures, and methods of combatable with the least expenditure of forces, to provide the greatest and most lasting results.'[56]

The commander is solely responsible for his decisions, as stated in the previous section of this paper, Principles and Methods of Troop Control. He is expected to calmly review the battle situation in terms of his dialectic methodology and then to "take" the "scientifically" correct decision.

> . . . profound knowledge of Marxist-Leninist dialectics, as the logic and theory of cognition, should lie at the basis of the commander's work method in decision taking.[57]

> On the basis of a thorough study of the situation data, the commander takes a decision, that is, works out a definite plan of combat under specific decisions.[58]

In order to make correct decisions in a timely manner, the commander relies on electronic equipment to order information, make it comprehensible, so that his decision time can be reliably decreased.

> Deciding to engage in combat is a commander's most important function. This work cannot be reduced to a simple thinking process, to considering the variants and to selecting the best one. Even a machine can handle these operations. The commander's decision is a social, emotional, and volitional act of enormous importance.[59]

> The automated control system will serve him [the commander] only as a means to select the best of all possible alternative decisions, but it always remains for the human being to make the decision and sanction it with social ideals and goals.[60]

Electronic equipment. Certainly wireless communications, radar, the use of satellites for reconnaissance, navigation, and communication, infrared and other imaging techniques, and a whole variety of other new technologies have revolutionized warfare and have brought new types and volumes of information into the control process. None of these is more important than the computer though, because only it can arrange this information explosion in an ordered manner quickly enough to allow decisions to be made in the short time frames necessitated by modern war. With the volume of information to be processed, man becomes a bottleneck in the decision-making process. The computer can overcome this bottleneck. The computer frees the commander from the tedious mathematical tasks of planning and operations: determining logistical needs, force ratios, and other calculations. This was pointed out in the section, Problems and Goals of Troop Control.

The computer serves three functions in the control process, acting as "consultant," "assistant," and "comrade-in-arms" to the commanding officer.

1) The consultant. In the consultant function, the computer is primarily a Data Retrieval System (DRS), constantly updated to give the commander the latest information on enemy and allied troop strength, geography and transportation infrastructure, location of units, availability of air power, ammunition stocks and the thousands of other facts relevant to war fighting. The consultant is a vital component of the commander's personal staff in Soviet troop control doctrine.

> It is essential that the commander personally (and not through delegated persons) use his own DRS, change programs and monitor the informational completeness of his consultant, treating it as a personal weapon, as a means of expanding his own memory and sensory organs. Only in this case can it be effective. Other key personnel may have their own small DRS of the same design, but with professionally oriented information.[61]

DRS systems should have their information constantly updated through interaction with other DRS.

> DRS, like people, should interact with themselves and with people in order to understand each other and continually renew their information resources.[62]

Finally, the consultant is part of an information system that parallels the human hierarchical chain-of-command, and is really only useful in so far as it is as a complete system linking together the various sources of information.

> A considerable advantage of the electronic consultant is the fact that it can be entrusted without danger to random thoughts, instantaneous ideas and considerations that appear promising; it does not distort or forget them, does not confuse the address and stores them until they can be developed, used or discarded. The consultative function of the automated complex should embrace all aspects of activity. When we speak of an automated complex we do not simply mean the DRS alone. We are talking about the entire set of automated systems that support military organizations. If only the commander has a DRS there is little to be gained: an isolated island of automation is nothing more than an exotic entourage in the complex technical equipment of an army.
>
> The strength of automation lies in the complex, the systems approach, and in interaction and mutual information.[63]

2) <u>The assistant</u>. Whereas in its consultant function the computer provides the commander with relevant information in the assistant function the computer helps to perform the tasks of decision preparation and decision-making by subjecting the information to predetermined analytic methodology. The assistant's functions are more specialized than the consultant's, with each assistant assigned to a staff function, and programmed with specific algorithmic software.

> In order to help the commander and his staff in the performance of these functions, it is necessary to develop a computer section and means of interaction between the automated complex and

> corresponding control links. Then the electronic assistant will be capable of independently working out proposals and justifying them. The decision to adopt or not to adopt these proposals is the responsibility of the commander or other key personnel. Proposals may pertain primarily to information decisions. Control of the parameters of the information decision preparation program (input of weight coefficients for various sources of information, limitations, etc.) is the responsibility of the operator, but all data processing and evaluation of the reliability of decision alternatives are entrusted to the electronic assistant.[64]

> The programs and data of the 'assistant' to a greater extent than of the 'consultant,' are individualized and specialized in accordance with the personal features of key personnel, character of the groups, and general arrangements made within a given group. The 'assistant' requires more continuous combat evaluation supplementing of programs, revision of old data, and continuous direct interaction. Cooperation between people and machines, just as between people at headquarters is essential.[65]

The intended result of the computerization of the decision-making process is to have all those tasks that can be regularized and systematized reduced to mathematic calculations done by computer. This frees the human commander from the tedious and time-consuming and enables him to spend more time on creative thought.

> The development of automation is aimed at the reassignment of information, computation and evaluation problems to computers. If an electronic assistant is available, the commander and the operators may direct almost all of their efforts into the creative channel since they have all the necessary data for this purpose and are not distracted by secondary problems.[66]

3) Comrade-in-arms. In this case the computer is used as a teaching-learning device. The use of the computer as comrade-in-arms is not very well developed at this stage according to Soviet writing on the subject but it is hoped that this function will be better developed.

> With high information communication channels, the electronic comrade-in-arms may service (at least through the computer channel) lower-level organizations. Therefore, the automated complex as a whole expands its comrade-in-arms functions

> to all organizations, in spite of the fact that the technical equipment of the lower-level control links may remain at a lower level for a long period of time. It is difficult to predict the future competence of the electronic comrade-in-arms and how great an influence it will have. It is clear, however, that a workable decision is always ensured, and that the creative energies of the commander and his staff will be liberated to the maximum extent from technological functions. Teaching and self-teaching of the comrade-in-arms, 'expansion of its thesaurus and programs will be accompanied by a general improvement of means of automation and development of group intellect.'[67]

Subordinate units (the troops). The new technologies are changing the nature of soldiery, placing new demands on the troops and creating a new class of soldier. As the principle of initiative and independence in the last section suggests, the troops must be made aware of the final objective of battle and the overall plan of action in case communication is cut off. This demands a high degree of training and indoctrination.

> Since a surprise attack is considered to be the most probable method for commencing military operations by the aggressor, consequently, the time for carrying out control measures (the time for readying the troops for combat) will be greatly limited.
>
> From this follows the indisputable conclusion that for the troops which are destined for combat immediately after the enemy attack, all control measures should be prepared ahead of time. Under this condition troop control with the onset of combat can be successfully carried out with brief signals. In the event of a break in communications with the superior chief, the subordinate commanders can begin to carry out the mission upon their own initiative, since they will be informed as to the overall purpose of the battle or operation.[68]

New types of soldiers are also developing from the revolution in military technology.

> The first group includes those who service automatic and automated control systems, engage in setting them up, monitor the precise operation of the equipment, carry out periodic servicing and repair work, eliminate malfunctions, and take care of unexpected emergencies. These are the engineering-

> technical and service-repair personnel. They are, so to speak, outside the framework of the automatic or automated control system and do not participate directly in its functioning. Of course, this does not diminish the significance of the work of those people; it is very important and directly ensures the combat readiness of our modern Armed Forces.
>
> Service personnel also perform intrasystem functions in automated control systems. In this case, the individual participates directly in the work of the control system as its leading element. Intrasystem functions are expressed in particular in operator labor, which is becoming increasingly common and encompasses all categories of fighting men. This type of military work is very demanding and sometimes requires maximum mobilization of a person's physical and mental capacities.
>
> The most important element of any type of [control system] is the commander. The appearance and development of automated troop control systems have increased rather than diminished the commander's role on the field of battle because the troop combat capabilities which the commander may use in battle have increased enormously. This has made control of battle more complex, and the commander has received an effective new means of control to optimize this process--the [automated control system].[69]

Scientific and technical progress in the control process is changing the background and make-up of Soviet military personnel.

> Up to 45 percent of the officer positions in the Armed Forces today are filled by engineers and technicians. Our military educational institutions may take pride in the fact that they were the first in the country to train specialists in computer technology and programmers.[70]

The Process of Automation

To the Soviets, military cybernetics--the use of computers in the control systems--has evolved considerably since its introduction to the Soviet Armed Forces in the 1950's. Joseph Douglass, one of the few American analysts who has worked on this subject and has published nonclassified materials, outlined three phases of automation in the control process. The first applications were the guidance systems of the early ballistic missiles, autopilots, and radar directed air defense missiles. The next was the use of computers to target and coordinate nuclear missile attacks. Douglass sees a third stage

emerging today with computers used as:

> . . . an adjunct to normal staff work in organizing combat and planning logistics supply.[71]

Soviet theorists conceive of the automation process as a continuum--with the functions of warfare previously the direct responsibility of man taken over by machinery--leaving man indirectly in control through the control system. If there is no mechanization of the control process, that is said to be "manual." Some mechanization makes the process "mechanized." If the control process can occur "without the direct involvement of man," it is "automated." When it is fully automated and all aspects of the control process except decision-making can occur without direct human intervention, the system is said to be "automatic."[72] But, the automatic control system does not dismiss the commander of responsibility in Soviet troop control doctrine.

> Therefore, automated systems of control over troop combat actions are not meant for fully automatic--that is independent of the human being--control of troop combat actions. No one has posed and no one is posing such a task for full automation of troop control.[73]

Soviet theorists see two stages of automation--"partial" followed by "full" automation:

> Partial automation 'covered control of small military units only, most often detached weapons units of small complexes such as, for example, an anti-aircraft missile batallion . . .'[74]
>
> Full automation . . . a process which encompasses the entire system of troop control or a broad area of it.[75]

The possibility of automation in any given area of the control system (or component "arm" of the Armed Forces) is seen to depend on these factors: the capacity of technology to meet the particular military control need, and the predisposition of a particular area of military affairs to the automation

of control [it's easier to automate missile forces and air defense].

> Conditions for automation of control are more complex in the ground forces. Human problems are the third category of factors:
>
> . . . it cannot be forgotten that troop control does not amount to simply controlling weapons systems. At all levels it is always the control of men and military collectives.
>
> The human factor has been and remains the basic factor in war.[76]

The Soviets see the automation process as part of a dialectic progression.

> The technical control devices which have been created and are being created due to scientific-technical progress, in turn themselves become one of the driving forces of this progress. They serve as the material base for automating amd mechanizing the control process.[77]

CONCLUSION

The Soviet doctrine of troop control touches nearly every phase of military activity and aspect of military science and art. This primer should have served to outline for the reader the basic considerations that constrain and/or enhance the use of control systems in modern warfare. Many phases and aspects related to control could not be covered in detail without significantly lengthening the paper and broadening its scope (i.e., the training and indoctrinate phases and the leadership aspect).

Soviet troop control doctrine is not a single line of thought; it is rather a collection of concepts which describe the nature of scientific-technical progress and their impact on war fighting--the "revolution in military affairs;" basic theoretical needs of and obstacles to troop control; the role of computers in decision-making; practical methods and principles of control; the relations between coordinating commanding bodies and their subordinate units, and the evolution of automation in the control system.

There is no strictly ordered doctrine but the collection of ideas that describe, order, and prescribe the state of warfare in the modern age are flexible enough to meet the situations that Soviet military commanders face.

Today in troop control doctrine there is no "father figure" theorist to pull the series of related concepts together in a single, comprehensive theory as Sokolovskii and Gorshkov have done for Soviet land and naval warfare doctrine.

This is perhaps because of the complexity of the control process, the as yet uncertain <u>final</u> effects of computers, satellites, and other modern technologies on that process, and the intimate interrelation of the control

process and all other facets of military activity. It has only been in the last few years that the American defense community has paid great attention to C3I, establishing as assistant secretary of defense for C3I, for example. The Soviets are probably undergoing a similar education process. If the classified data on Soviet C3I systems were made public, I would be better aware of just how far along on the learning curve they are.

One thing is certain; Soviet military doctrine embraces the use of modern technical means wholeheartedly. In the past we have seen them in the area of weapons deployment attempts to adapt the latest technology to weapons as quickly as they possibly can. The nature of their command economy ensures that they are not significantly behind the West in state-of-the-art sophistication and may in some cases be ahead of their Western counterparts. The emergence of a theoretical work that ties the series of concepts (mentioned above) together--and an author of the stature of Gorshkov or Sokolovskii--will be a sure warning that the Soviet military has decided on a course of control system deployments and have, at least, theoretically resolved the true effect of the new electronic environment on war fighting.

NOTES

1. Col. Gen. N. A. Lomov, "Introduction" from The Revolution in Military Affairs (RMA), Moscow, 1973, translated and published under the auspices of the USAF Soviet Military Thought Series (SMTS), number 3, p. 2.

2. Ibid., p. 6.

3. Ibid., p. 5.

4. V. D. Sokolovskii, Soviet Military Strategy, Moscow 1963, translated by Herbert Dinerstein, Leon Gouré, and Thomas Wolfe, p. 295.

5. Ibid.

6. Ibid., p. 301.

7. Ibid., p. 302.

8. Ibid., p. 296.

9. Maj. Gen. A. Ye Tartarchenko, "The Increase in the Role of Troop Control in Modern Combat" from RMA, p. 165.

10. Ibid., p. 164.

11. Ibid., pp. 165-166.

12. Adm. Gorshkov, The Sea Power of the State, Naval Institute Press, Annapolis, MD., 1979, p. 209.

13. V. V. Druzhinin, D. S. Kontorov, Concept, Algorithm, Decision (CAD), Moscow, 1972, translated and published under the auspices of the USAF, SMTS number 6, p. 3.

14. V. M. Bondarenko, "Scientific-Technical Progress and Troop Control" from Selected Soviet Military Writings: 1970-1975 translated and published under the auspices of the USAF, SMTS number 11, p. 225.

15. Tartarchenko, p. 173.

16. Bondarenko, p. 226.

17. Gen. S. M. Shtemenko, "Introduction to the Russian Edition" from CAD, p. 3.

18. Shtemenko, p. 2.

19. Ibid.

20. Ibid., p. 4.

21. Druzhinin, Kontorov, p. 7.

22. Ibid., p. 10.

23. Ibid., p. 11.

24. Ibid.

25. Tartarchenko, p. 175.

26. Druzhinin, Kontorov, p. 16.

27. Ibid., p. 257.

28. Ibid., pp. 265-266.

29. Tartarchenko, p. 164.

30. Maj. Gen. A. K. Zaporozhchenko, "Principles of Troop Control in the Combat Process," from RMA, p. 180.

31. Bondarenko, p. 181.

32. Ibid., p. 182.

33. Sokolovskii, p. 457.

34. Ibid.

35. Ibid., p. 458.

36. Ibid.

37. Tartarchenko, p. 164.

38. Ibid., p. 165.

39. Ibid., p. 165.

40. Zaporozhchenko, p. 168.

41. Ibid., p. 169.

42. Ibid.

43. Ibid.

44. Ibid.

45. Ibid., p. 170.

46. Ibid.

47. Ibid.

48. Ibid., pp. 170-171.

49. Ibid., p. 171.

50. Ibid.

51. Ibid.

52. Ibid., pp. 171-172.

53. Ibid., p. 172.

54. Ibid.

55. Ibid.

56. Galkin, "The Revolution in Military Affairs and the Increased Role of Science in Troop Leadership," from RMA, pp. 220-221.

57. Zaporozhchenko, p. 184.

58. Ibid.

59. Bondarenko, p. 231.

60. Ibid., p. 232.

61. Druzhinin, Kontorov, p. 285.

62. Ibid.

63. Ibid., pp. 285-286.

64. Ibid., pp. 287-288.

65. Ibid., p. 288.

66. Ibid.

67. Lomov, "Conclusion" from RMA, p. 293.

68. Zaporozhchenko, p. 186.

69. Bondarenko, p. 232.

70. Ibid., p. 228.

71. Joseph D. Douglass, Jr. The Soviet Theatre Nucelar Offensive, published under the auspices of the USAF, GPO, Washington, D.C., p. 84.

72. Druzhinin, Kontorov, p. 174.

73. Bondarenko, p. 231.

74. Ibid., pp. 229-230.

75. Ibid., p. 231.

76. Ibid., p. 230.

77. Druzhinin, Kontorov, p. 175.

BIBLIOGRAPHY

Bondarenko, V. M. "Scientific-Technical Progress and Troop Control" in Selected Soviet Military Writings 1970-1975; translated and published under the auspices of the USAF, USGPO, Washington, D.C., 1978.

Douglass, Joseph D., Jr. The Soviet Theatre Nuclear Offensive, published under the auspices of the USAF, USGPO, Washington, D.C., 1977.

Druzhinin, V. V. and Kontorov, D. S. Concept, Algorithm, Decision (CAD) Moscow, 1972; translated and published under the auspices of the USAF, USGPO, Washington, D.C.

Galkin, M. I. "The Revolution in Military Affairs and the Increased Role of Troop Leadership" in The Revolution of Military Affairs (RMA), Moscow, 1973; translated and published under the auspices of the USAF, USGPO, Washington, D.C.

Gorshkov, The Sea Power of the State, Naval Institute Press, Annapolis, MD.

Lomov, N. A. "Introduction" and "Conclusion" in RMA.

Sheldon, Charles G. II. "Chapter Six--Soviet Military Space Activities" in Soviet Space Programs, 1971-1975, a staff report prepared for the Committee on Aeronautical and Space Sciences of the U.S. Senate by the Science Policy Research Division of the Congressional Research Service, USGPO, Washington, D.C., 1960.

_____. "United States and Soviet Progress in Space: Summary Data through 1979 and a Forward Look." Congressional Research Service, Washington, D.C. 1978, revised 1980.

Shtemenko, S. M. "Foreword" to CAD.

Sokolovskii, Soviet Military Strategy, Moscow, 1963, translated by Herbert Dinerstein, Leon Gouré, and Thomas Wolfe.

Tartarchenko, A. Ye. "The Increase in the Role of Troop Control in Modern Combat," in RMA.

Zaporozhchenko, A. K. "Principles of Troop Control in the Combat Process," in RMA.

CRISIS MANAGEMENT AT EXXON CORPORATION

George N. Curuby
92 Kensington Lane
Swampscott, MA 01907
December 11, 1980

TABLE OF CONTENTS

SUMMARY OF FINDINGS

The aim of this paper is to assess Exxon's ability to respond to two of the threats faced by international oil companies today: a sudden, major cutback of oil from Saudi Arabia and military action in the Persian Gulf. Exxon was chosen because it has one of the most sophisticated oil management capabilities in the industry as well as a unique data processing system for supply planning and tanker fleet scheduling. In order to understand how Exxon might respond to a future crisis, this paper examines the company's experience during the 1973 Arab oil embargo and the period following the storming of the mosque in Mecca in the Fall of 1979. Most of the analysis is based on interviews conducted at Exxon prior to the war between Iraq and Iran. However, it offers insights into how Exxon is now responding to the shutdown of oil production in those two countries and to the threat to shipping in the Persian Gulf.

Three conclusions are drawn in this study. First, in the operations area Exxon is able to adjust quickly to unexpected production cutbacks with existing procedures. However, it is vulnerable to shortages caused by tankers being unable to unload at major refineries. Second, while the Transportation Operations Division (TOD) can communicate with Exxon's tankers during a crisis, it has difficulty obtaining the tactical information necessary to make command decisions. In part, this is due to the way information is organized within the company, and in part to the problem of obtaining precise information from government officials. Third, while the company can expect increased government intervention in the event of a supply shortage more serious than previous ones, the lack of oil more than the intervention itself will constrain the company's ability to allocate the remaining supplies.

INTRODUCTION

In 1973, Aramco (The Arabian American Oil Company) was owned by four major oil companies and the Saudi Arabian government. Exxon, Socal, and Texaco each held 22.5 percent of the shares of the company, Mobil 7.5 percent, and the Saudi Arabian government 25 percent. The companies had submitted to Saudi pressure in 1972 by selling it shares, and had agreed that the government would increase its percentage to 51 percent by 1982. However, in reality the Saudi government had physical control of the oil.

Prior to the Arab oil embargo, the Exxon system was crude short. Both the Saudi Arabian and Venezuelan governments had recently taken control of crude production levels which accounted for two-thirds of Exxon's supplies. After discussions at Exxon about how this constrained company decision-making, the general opinion was that the existing operating procedures for supply planning and allocation were adequate to meet any foreseeable contingency. The 1973 embargo tested this assumption and proved it was basically correct.

Today, faith continues in Exxon's ability to allocate oil within its system and to command and control the tanker fleet in times of crisis. After spending a day at Exxon, I was reasonably convinced that this faith is well founded. However, with my elementary understanding of Exxon's operating procedures, I would like to examine their ability to respond to crises because I was told by executives during my visit: "We don't spend much time wondering, 'What if?' because too many 'What ifs' can occur. We do recognize the many variables and try to remain as flexible as possible to deal with them." To the extent that this analysis identifies operational problems of the oil business, I hope it furthers the understanding of

command, control and communications as they apply to a multinational enterprise.

ARAMCO'S INITIAL RESPONSE TO THE ARAB OIL EMBARGO

The Arab oil embargo began on October 18, 1973 when Radio Riyadh announced an immediate 10 percent reduction in Saudi Arabian oil production. An Aramco employee called up Frank Jungers, Aramco's chairman, and told him the news. Without asking for further details and without contacting the Aramco partners, Jungers ordered the wellheads shut in to accommodate the reduction. He later said, "The important thing was to give the immediate image of being with the government, not trying to fight it."[1]

Four days later, a local bureaucrat informed the Aramco controller that a meeting was scheduled that afternoon at the Oil Ministry.[2] From that meeting until the end of the crisis, the Saudi government made the decisions regarding the allocation of Armaco's oil. One Exxon executive has suggested that Aramco officials avoided direct contact with the government for four days in order to retain as much operating flexibility as possible. However, the lack of precise information delayed some of the operational and tactical decisions which Aramco and the partners had to make.

The way the partners decided upon the level of Aramco's production was historically a matter of dispute. An arrangement had been worked out whereby partners could "over-lift" the oil not wanted by the others. But as a result of the production cutback, the partners started to demand their full shares of oil under the Aramco agreement. At first they argued over who could deliver the oil to the unembargoed countries. This disagreement caused minor delays in the allocation of Saudi crude. However, it was the

addition of country-specific embargoes to the cutbacks which complicated the distribution of crude and created the real organizational problems during the embargo.

For one week following the first announcement, there was confusion at Aramco's offices in Dhahran. Until that time, Aramco had paid little attention to where its shareholders delivered the oil. But, this information became critical in determining how much each partner would be allowed to ship to each country. Clerks in Dhahran searched through thousands of billings, tracking down the companies' previous deliveries to 68 countries. From the billings, Aramco worked out new monthly quotas for each partner, country-by-country, and in effect administered the cutback.[3]

EXXON'S RELATIONSHIP WITH ARAMCO TODAY

While Exxon relies on Aramco's facilities for producing and loading crude from Saudi Arabia, Exxon executives concede that in terms of operations the Saudi government has complete control of Aramco. In spite of a close relationship between Exxon and Aramco, the integration between the two at the operations level has needed improvement. Aramco is now in the process of being connected with Exxon's computerized supply scheduling system (the LOGICS system) which will facilitate the processing of Exxon's changes in crude oil and tanker movements from Saudi Arabia. This promises to help solve the scheduling problems which could arise during another supply crisis. During the 1973 embargo, Exxon executives claim that they were able to process the changes in oil movements created by the selective embargoes with the LOGICS system. The Aramco clerks in Dhahran, lacking the same data management system, had a more difficult time. An examination

of how Exxon schedules and monitors the movement of oil will show why Exxon's supply scheduling system worked smoothly during the crisis.

SUPPLY PLANNING AT EXXON

Exxon has six regional affiliates (Esso East, Esso Europe, Esso Middle East, Esso Inter America, Exxon USA and Imperial Oil in Canada) which are divided along functional lines of production, refining and marketing. Worldwide supply plans are formulated through an interaction between Exxon International (EIC) and Exxon's affiliates. EIC presents the refining and marketing affiliates with its preliminary determination of the availability and prices of crude oil and petroleum products. Each affiliate puts together its own estimates of sales and demand for each country which are then assembled on a regional basis and sent to EIC. At the same time, the affiliates who are producers send their estimates of available crude to EIC which in turn gives them preliminary estimates of projected demand within the system.

Once EIC determines how much oil is available and what the demands of the refining and marketing affiliates are, it draws up a worldwide supply plan. Formerly, EIC made these plans on a six-month basis. Currently, they are done every three months because of rapidly changing world conditions. This plan is discussed among the supply managers of the regional affiliates during meetings in New York. When a final plan is agreed on, it serves as a basis for the monthly operations supply plan.

Twenty days before each month, the affiliates send estimates of their demands or supplies for the upcoming month (which have been agreed to in the worldwide plan) to the Supply and Transportation Department (S&T).

They are sorted out by S&T which matches crude types with refinery needs and shipment sizes with tankers. Ten days before the month a preliminary scheduling plan is sent back to the affiliates who then advise S&T of any desired changes. By the first of the month a scheduling plan is finalized which serves as the base plan for the month.

This operations supply plan is formulated and executed with the help of an oil vessel data management system called LOGICS. The needs of the regional affiliates are entered into the LOGICS system as specified for arrival at a given port within a certain date range. The Supply Division, a part of S&T, looks at the needs and enters on the system the volumes of crude they expect to be able to supply. The regions check their data terminals to see how their requests will be satisfied and make adjustments.

At about the same time, the Transportation Operations Division (TOD), also a part of S&T, examines the data to determine the assignment of vessels to move the oil. When decisions on oil allocation have been made, vessels are matched with specific crude needs. Once the Supply Division has confirmed supplies, unilateral changes by the TOD are not permitted. LOGICS automatically notifies the Supply Division whenever a loading date needs to be changed, for example if for some reason a vessel is delayed. The LOGICS system retains the data on the prior schedule until a change is accepted by the Supply Division.

Within the LOGICS system is a Vessel Control sub-system which monitors and continually revises the itineraries of the Exxon-controlled fleet of 137 vessels. Once the TOD has decided which vessel will be used to move a shipment of crude, the name of the vessel is typed into the system. Seconds later, the itinerary of the vessel is displayed on the screen. The sub-system plots the voyage, considering load ports, discharge ports, vessel

speeds, canals and the vessel's route. It takes into account when the crude supplies are available, when they need to be delivered, and then plots the return voyage of the vessel to the next assigned area so that the TOD will know when it is next available. Once the voyage has been created the sub-system will replot the itinerary and adjust subsequent voyages if any change occurs.

EXXON'S RESPONSE TO A PRODUCTION CUTBACK

A sharp production cutback in Saudi Arabia, for example, is not an immediate shock to the Exxon system. There is normally a 30-40 day period from the time a tanker loads crude oil at the port of Ras Tanura to the time it arrives at a refinery in Europe or the Mexican Gulf. Therefore, Exxon's refining and marketing affiliates do not immediately experience the cutback and have time to adjust.

As soon as the news of a cutback reaches S&T, the TOD instructs the vessels at the loading facilities to continue loading and the vessels heading toward the facilities to slow down. Meanwhile, estimates of the shortage are sent by the Supply Division to the affiliates so that they can begin gearing down their operations. The affiliates know, based on experience, approximately how much a cutback will impact on them and the Exxon system.

If a refinery is set up to process one of the several types of Arabian crude, the Cargo Department will buy on the open market or swap the particular crude with another company. If it is not available, the refineries know before they experience the cutback to conserve their existing supplies and to spread them evenly over the shortage period. There is a great deal of common sense involved in this adjustment process.

Just as the refineries have a grace period, EIC has time to determine what actions to take. For the time being, the affiliates operate as closely as possible to the existing monthly plan. Those vessels already en route continue as planned. Meanwhile, EIC has the opportunity to assess the severity and duration of the cutback, communicate with the affiliates, and work out a new supply plan. Once this new plan is finalized, the affiliates and S&T work out a new scheduling and transportation plan.

LOGICS has improved Exxon's ability to respond to a sharp cutback. Since 1973, two additional affiliates, Esso East and Esso Inter America, have been tied into the system. As mentioned, Aramco is in the process of being connected. This gives S&T increased ability to process scheduling changes, and makes it more unlikely that this area would become a bottle-neck following a production cutback.

EXXON'S IMMEDIATE SUPPLY PROBLEM

While S&T has time to respond to a production cutback, there is a supply shortage which requires immediate action. In the event a docking facility of a major refinery suffers damage and supertankers are unable to unload, the refinery may be forced to rapidly cut production. This is particularly true if the Exxon system is crude-short and the refinery is operating with limited reserves. The refinery at Aruba experienced this problem and caused a minor crisis.

Depending on the season and the reserves at hand, the inability of a supertanker to offload can have an immediate impact on a major refinery and consequently an entire region. While this situation is normally short-lived, Exxon can do little more than repair the damage quickly. For example,

even if the oil could be offloaded onto smaller tankers and brought to other refineries in the region, those refineries may not be able to handle that particular type of crude. Or markets may not exist near the refineries for the products which are made from that crude. Thus, if the docking facilities at a major refinery are out of service for a period of time, Exxon will experience greater stress than it will from a production cutback of a similar duration because the loss of supply is localized in the region. And unlike a production loss, the shortage cannot be allocated rapidly throughout the entire system.

MILITARY ACTION IN THE PERSIAN GULF

In the course of normal operations, the TOD maintains regular contact with its ships via telex and receives routine messages of vessel positions which are fed into the Vessel Control sub-system. Satellite communications equipment is being installed on all vessels coming in for their biannual overhaul. However, the TOD does not believe it is necessary for the entire fleet to have this equipment for command and control purposes.

In the event of a crisis, it is standard procedure for the TOD to send a telex to the vessels of the fleet putting them on alert and informing them of the situation. While on alert, the masters proceed with caution pending further instructions, and have the authority to override prior instructions from the TOD if they feel it is necessary. Thus, the masters are authorized to make tactical decisions while on alert until the TOD instructs them what actions the fleet should take.

During the communications blackout in Saudi Arabia which followed the storming of the mosque in Mecca in the Fall of 1979, the TOD was able to

communicate with the masters of vessels at the loading facilities at Ras Tanura via satellite. The masters, in turn, spoke by radio with Exxon's shipping agent and Aramco personnel to learn what they could about what was happening on shore. Since there was no sign of hostilities, loading activities did not stop. However, the masters kept close watch of the shore with binoculars and were told to set sail at whatever point they felt the safety of their ships was in danger.

Following the blackout, the TOD became concerned about maintaining communications with its fleet during another crisis. It examined nine alternative telex routes to the Gulf in case normal communications channels to Bahrain were blacked out, and from these chose three. With these tests, the TOD believed the communications capability with its ships in the Gulf was adequate in the event of another crisis.

After President Carter declared his intention to blockade Iran on May 11, 1980, the TOD prepared a plan for its tankers in the event hostilities broke out in the Persian Gulf. First, tankers approaching the Gulf were to proceed to ports which the TOD selected where supplies and bunker fuel would be available in the event of a long period of conflict. Second, all vessels were to be put on alert according to normal procedures and masters of vessels in the Gulf were to take immediate actions to ensure their vessels' safety. These basic emergency procedures were backed up with the communications plan.

While the TOD was satisfied with its preparations for a May 11 blockade, one problem remained. During the communications blackout, the TOD was delayed in issuing commands to the fleet because obtaining the information necessary to make tactical decisions proved to be difficult. As a result, even though the TOD was able to communicate with the fleet, tactical

instructions were not issued for a number of days. This difficulty in obtaining the information necessary to make operational decisions is experienced by other departments within Exxon as well.

POLITICAL INTELLIGENCE

At Exxon, the affiliates collect most of the company's political intelligence and are considered the best sources of this information because of their close contact with governments and customers. There is no staff in EIC which tries to analyze the political situation on a country-by-country basis. So, EIC relies to a significant extent on the public affairs department, which in turn relies on the affiliate in each country.

The public affairs department is involved with long-range political assessments as well as with the day-to-day information obtained by the affiliates. It performs in-depth studies of countries which are Exxon's major sources of supplies, countries in which large investments are contemplated, and countries outside the normal concern of the affiliates. Otherwise, the affiliates do most of the environmental risk assessment.

A recent issue of Fortune magazine states that "Exxon goes further than most corporations by integrating its political assessments into financial plans. Exxon compares its vast intelligence with views from a panel of outside experts on the country. So far, Exxon has avoided rude shocks by getting sophisticated appraisals through its regional divisions, the hubs of corporate intelligence. Richard Barham, Esso Middle East's government relations advisor said, 'We never accept their reports at face value, but check them with many other sources.'"[4]

An executive in the public affairs office estimates that 90 percent of the information flow is routine. However, during a crisis, "We go anywhere

we can to get the information we need."[5] For example, during the communications blackout in Saudi Arabia, phone calls were made in all directions--S&T to Esso Middle East, public affairs to the State Department, Esso Middle East to the Department of Defense, public affairs to Esso Middle East, S&T to public affairs, etc. Never accepting reports at face value, but checking them with many other sources is the rule even during periods such as this.

However, at the operations level and in the public affairs department, a similar problem is experienced: "Often times you call the government and they're fuzzy, they don't give you a real answer."[6] It is even more difficult for someone at Exxon to determine what is US policy. "The government wants to retain its flexibility, especially in the areas of petroleum and international affairs, so no answer is definite."[7] At the same time, Exxon officials don't want to push too hard for an answer, or make an official take a position which might adversely affect the company.

There is a greater need to obtain information and more reluctance to force statements from foreign governments. The four days in 1973 during which Aramco did not communicate with the Saudi government is a good example. If during a crisis the managers of the affiliates are reluctant to press their host governments for information (and if the US government is at best only fuzzy), the operations level which needs to make tactical decisions suffers delays. In the future this may have serious consequences.

CORPORATE DECISION-MAKING DURING AN ACUTE SUPPLY SHORTAGE

During the 1973 embargo, Exxon operated within two types of restrictions: political concerns and technical constraints. Political concerns related to consuming countries, especially those that were given preferred access to

oil by the Saudi government. Exxon needed to justify not giving those countries more crude than was necessary because it was short of oil on a worldwide basis. Technical constraints included the limited ability of refineries to process different types of crude, the lack of markets for some products which were able to be refined in other areas, and the lack of deep water ports in the United States for supertankers.

At Exxon and in the oil industry, there was a widespread belief that failure to redistribute supplies equitably would invite increased government intervention. Therefore, Exxon made great efforts to convince consuming governments that the pain was being spread evenly.[8] Two formulas were decided on to allocate crude oil among consuming countries. One was based on the percentage of each affiliate's regional demand during a base period. The other was based on a forward supply plan that was made before the crisis. The objective was not to allocate crude oil and refined products on a profit-maximizing basis, but rather "to allocate on what we thought was a fair and equitable basis."[9]

Following the revolution in Iran, Exxon justified its allocation decisions by sticking closely to the international Energy Agency plan for allocating acute shortages which the major consuming countries had formulated after the 1973 crisis. While Exxon and the other oil companies experienced political pressure during this period, they avoided government intervention in their corporate decision-making. The question remains whether a more serious shortage, for example a shutdown of Aramco whose current output is 9.5 million barrels a day or 20 percent of the total free world supply, would bring about direct government participation in decisions regarding the distribution of the remaining oil.

Exxon executives doubt that the United States government has a contingency plan for a cutoff of oil from Saudi Arabia. They feel that there is little the government can do other than force increased domestic production and maximize conservation. If such a plan exists, it is not coordinated with the companies which produce, transport, or supply the oil. It is unclear whether coordinating at this point would avoid more direct government intervention in the future. However, at present there is little to coordinate since Exxon has no contingency plan, largely because executives believe the company has few options if Saudi Arabia's production is lost.

In an issue of Oil and Gas Journal prior to the 1973 embargo, Kenneth Jamieson, chairman of Exxon, said that petroleum is a business of international management, and cited the oil companies' ability to handle international oil traffic.[10] Judging from the way Exxon responded to the 1973 embargo and to the Iranian crisis, it seems that this capability is still in place. The ways in which the consuming governments will constrain this capability in the event of a more acute supply shortage is open to speculation. However, if the shortage is acute enough to cause government intervention, it is likely that the lack of oil to distribute will be more of a constraint on corporate decision-making than any actions which the governments may take.

NOTES

1. Demaree, Allan T., "Aramco is a Lesson in the Management of Chaos," Fortune, February 1974, p. 58.

2. Ibid., p. 63.

3. Ibid., p. 64.

4. Fortune, March 24, 1980, p. 88.

5. _____, Based on an interview conducted at Exxon Corporation in New York, April 25, 1980.

6. Ibid.

7. Ibid.

8. Comments by an Exxon executive in a speech at Harvard, Spring 1980.

9. Ibid.

10. Oil and Gas Journal, April 30, 1975, p. 95.

BIBLIOGRAPHY

Baltic International Maritime Council, Bulletin V-1979, "Shipborne Navigational Equipment," p. 4813.

Baltic International Maritime Council, Bulletin V-1979, "Inmarsat, a New Communications System for World Shipping," p. 5310.

Bes, J., Tanker Shipping: Practical Guide to the Subject for All Concerned with the Tanker Business, Amsterdam, 1963, pp. 234-239.

Business Week, "A New Face for Exxon's New Role in Oil," July 14, 1975, p. 136.

Demaree, Allan T., "Aramco is a Lesson in the Management of Chaos," Fortune, February 1974, p. 58.

Exxon, Annual Reports, 1974, 1975, 1976, 1977, 1978, 1979.

Exxon Background Series, "Middle East Oil," EBS 8/76.

Exxon Background Series, "Tankers and the Flags They Fly," June 1979.

Exxon Background Series, "Very Large Crude Carriers," EBS 11/75.

Forbes, "Exxon Corporation," April 1, 1973, p. 30.

Fortune, March 24, 1980, p. 88.

Freight Management, "Esso's Packaged Goods Distribution," September 1977, p. 46.

Inter Governmental Maritime Organization, Merchant Ship Position-Reporting Systems, London, 1971.

International Management, September 1974, p. 14.

Milano, James and Grub, Phillip, "Developing a Worldwide Corporate Information and Control System: Problems and Guidelines, in Sethi and Holton, eds. International Accounting and Information Systems, New York,1974, pp. 317-325.

Moreby, David, The Human Element in Shipping, Seatrade, 1975.

Mosel, Noel, Supertanker, Viking, 1975.

Oil and Gas Journal, "Exxon, No Confrontation Please," April 30, 1973, p. 95.

Oil and Gas Journal, "International Oil, learning to adjust to the new world," April 29, 1974, p. 11.

Robock, S., Simmonds, K. and Zwiek, J., International Business and Multinational Enterprise, pp. 517-523.

Tanaka, R., "The Maritime Mobile Service, its functions and constitution," Telecommunications Journal, vol. 44, V/1977, p. 239.

Telecommunications Journal, "Mobile Radiocommunications," vol. 45, VII/1978, p. 385.

Telecommunications Journal, "Telecommunications Services for Small Vessels in Greek Waters," vol. 44, V/1977, p. 236.

Telephony, "Petroleum giant orders ITT's switch to speed International Communications," June 25, 1979, p. 58.

Wolgast, A.K., Transcript of a speech made at Harvard, March 25, 1980.

Copy 1