

Modernizing Intelligence: Structure and Change for the 21st Century

with

**A Note from LTG William E. Odom, USA (ret)
Study Chairman**

edited by
Bernard C. Victory

January 2002 Edition

National Institute for Public Policy

3031 Javier Road, Suite 300 • Fairfax, VA 22031 • (703) 698-0563 • www.nipp.org

The National Institute for Public Policy is a nonprofit corporation founded in 1981 to promote public education on international issues. National Institute study efforts address a range of topics in national security affairs, including U.S.-Russian relations, weapons proliferation, ballistic missile defense, deterrence theory, long-range air power, and intelligence reform.

In addition to this research, the work of National Institute includes a number of other activities. The Institute sponsors the international journal, *Comparative Strategy*, organizes conferences and seminars on various national security issues, and publishes a series of publicly available reports on defense-related topics. *Modernizing Intelligence: Structure and Change for the 21st Century with a Note from the Study Chairman* is the latest in this series. This publication updates the report *Modernizing Intelligence: Structure and Change for the 21st Century*, September 1997.

The programs of National Institute are supported by government, corporate, and private foundation grants and contracts. The views expressed in this report do not necessarily reflect the view of National Institute for Public Policy or any of its sponsors.

Additional copies of this report are available for \$15.00 each from the National Institute for Public Policy, 3031 Javier Road, Fairfax, VA 22043, (703) 698-0563.

© National Institute for Public Policy, 2002
www.nipp.org

The CIA's Publications Review Board has reviewed this report to assist in eliminating classified information, and poses no security objection to its publication. This review should not be construed as an official release of information, confirmation of the report's accuracy, or an endorsement of its views.

Modernizing Intelligence: Structure and Change for the 21st Century

Study Chairman:

LTG William E. Odom, USA (ret.)

Senior Advisory Group:

Dr. William R. Graham

Mr. Robert E. Rich

Ms. Elizabeth R. Rindskopf, Esq.

Lt. Gen. Harry E. Soyster, USA (ret.)

Dr. Gregory Treverton

Lt. Gen. James R. Clapper, USAF (ret.)

edited by
Mr. Bernard C. Victory

Modernizing Intelligence: Structure and Change for the 21st Century

Table of Contents

A Note from the Study Chairman.....	v
Preface.....	xi
List of Abbreviations.....	xiii
Executive Summary.....	xvii
Section I. Introduction: Why Intelligence Community Reform?	1
Section II. Principles and Concepts for Intelligence Organization, Operations, Management, and Training.....	7
Section III. The DCI Management Structure for the Intelligence Community	31
Section IV. The Defense Department's Intelligence Structure: A Review and Recommendations for Reform	51
Section V. The Signals Intelligence Discipline: Structure and Management	69
Section VI. The Imagery Intelligence Discipline: Structure and Management	79
Section VII. The HUMINT Discipline: Review and Recommendations	85
Section VIII. Counterintelligence.....	99
Section IX. Conclusion.....	109
Appendix A Description of the Intelligence Process, and the Organizations Discussed in this Study	113
Biographies	123

This study was begun in late 1995 and first published in 1997. As it asserted, the Intelligence Community was in serious need of major structural changes, not simply policy changes and more or less funding. Few organizations, either in the government or the private sector, have experienced as much infusion of changing technologies, such ups and downs in funding, and as many changes in the kinds and substance of the products they must provide. Private sector organizations experiencing such changes, which were not dramatically restructured, have not performed well. AT&T, General Motors, and RCA are examples. IBM almost waited too long before taking adequate restructuring measures. Even without examining the Intelligence Community, therefore, the presumption in 1997 had to be that restructuring was overdue.

Calling for major change, especially in government bureaucracies, is never met with welcome or applause. That was the case with this study, but its arguments and analysis were never openly challenged. Still, the study has received fairly wide readership—if requests for copies are an index. The first printing has been sold out for over a year. It also caught the attention of several foreign governments friendly to the United States, and one of them appointed a commission to review its own intelligence structures, using this study as a guide for its work, and discussing organizational issues with at least one member of the study group. For that reason, the National Institution for Public Policy, in cooperation with the Hudson Institute, is publishing this second edition.

The recommendations of the original study have stood up well over the past five years. Instead of rewriting the text, therefore, it seemed more useful to review what has happened in the Intelligence Community in the intervening five years and to judge those developments against the conclusions and recommendations of the study. To that end, three questions have been posed:

- What structural changes have been made in the Intelligence Community?
- What major problems did the study overlook in light of subsequent developments?
- What has happened that vindicates the study's analysis and recommendations?

These questions form the outline for the remainder of this note.

Structural Changes

Only one of the major structural changes recommended by this study has been partially implemented: the creation of the National Imagery and Mapping Agency (NIMA). NIMA was officially formed shortly before the study was completed, and the idea of such an agency was suggested in open hearings held by the Senate Select Committee on Intelligence under the chairmanship of Senator David Boren in the late 1980s (See p. 2.). Boren subsequently proposed that an imagery agency be created in his draft legislation for intelligence reforms, but the idea languished for several years until John Deutch became the Director of Central Intelligence. During his tenure NIMA was founded. As this study warned (see pp. 82-84), making

NIMA effective would not be easy, and it would require much support from the top levels of the Defense Department and the military services.

Unfortunately, not only did high-level support not materialize to the degree required, but a related, recommended structural change did not accompany NIMA's creation: splitting the National Reconnaissance Office and making its imagery program offices an R&D and procurement arm of NIMA (and the signals intelligence program offices an R&D and procurement arm of NSA). Not only were the NRO program offices not transferred to NIMA, the NRO and CIA kept some operational control over national imagery systems. NIMA, therefore, has not enjoyed an auspicious start.

Problems Overlooked

The National Security Agency (NSA) has had major internal problems, some due to the rapidly changing communications technologies in the world, others due to the post-Cold War reductions in budgets and personnel. Although the challenge of keeping ahead of technological change and related matters were flagged by the study as potential problem areas needing the DCI's attention and outside scrutiny (see p. 76, recommendation No. 3 and discussion), these problems have turned out to be far more severe than the study suggested. More specifically, they were not flagged as so urgent and serious as they were at the time or would soon become. Prompted by investigations by the House Permanent Select Committee on Intelligence, the complete breakdown of NSA's central telecommunications center for three days, and troubling personnel problems, NSA has had to confront a backlog of accumulating difficulties. Much effort, reportedly, has already been made to cope with them.

Perhaps there have been other major problems not anticipated at all or sufficiently in the study, but beyond the case of NSA, they have not been conspicuous.

Problems Identified That Remain Unaddressed

Counterintelligence. The study put heavy emphasis on the deficiencies of the CI system (See Section VIII, pp. 99-107). Fragmentation of CI responsibilities leaves large gaps for hostile penetrations, and the mixing of criminal law enforcement responsibilities with CI responsibilities in the same organization ensures that CI skills will suffer and resources remain inadequate. The solutions to these problems require major changes in organizational responsibilities, beginning with relieving the FBI of its entire CI mission and transferring it to a newly created National Counterintelligence System (NCIS) under the Director of Central Intelligence (DCI).

The weakness of the Intelligence Community's CI capabilities was painfully apparent when the study was published. Aldrich Ames had been uncovered as a Soviet and Russian agent within the CIA. Since then, Robert Hanssen of the FBI was discovered to be a long-time Soviet and Russian agent. Several less damaging agents have also been discovered since 1997. The resulting picture is one of general transparency of the US Intelligence Community—its capabilities, operations, and findings—to the Soviet Union and (after 1991) Russia. Other hostile intelligence services can be assumed to have significant penetrations as well. If the intelligence capabilities of non-state organizations such as al-Qaeda are included, then the attacks on the World Trade Center and the Pentagon show that US Counterintelligence is

tragically weak. So too, of course, do these terrorist attacks reflect badly on the entire Intelligence Community, especially NSA and the CIA/DO.

The public discussion of the Ames and Hanssen cases gave the impression that they were major exceptions, that such penetrations are extremely rare and unusual. Some critics blamed the Church and Pike committees in the Congress for weakening the IC in the 1970s as an explanation of such staggering damage. Would that things were only that bad. If one takes a long historical view, the reality is far worse.

The FBI belatedly created an office focused on the Soviet espionage in 1943. During the 1920s and 1930s, when the Communist International (Comintern) was creating Communist parties throughout the world, the FBI remained remarkably disinterested in that development. The NKVD (predecessor to the KGB) had already entrenched its agents widely within the United States in general and inside the government in particular by 1943 when the FBI belatedly became interested. Two recent books published by Yale University Press—*The Secret World of American Communism* and *The Soviet World of American Communism*—reveal that the American Communist Party and its Comintern umbrella in Moscow were able to evade, confuse, and otherwise neutralize US counterintelligence throughout the interwar years, during the war, and into the postwar period. The Venona file, declassified by NSA, reveals equally damaging information. Over 240 Americans were named in messages to Moscow by Soviet agents. Despite this massive tip-off, the FBI was unable—or unwilling—to sustain surveillance of these suspects until sufficient evidence was collected to ensure successful prosecutions in court. Thus they were allowed to operate with impunity.

If a close study were made of all the espionage cases reported and unresolved or failed in prosecutions in court since 1940, using the FBI, CIA, and military services' CI classified files, this picture would probably become all the more dismal. Felix Bloch, for example, was a US Foreign Service officer discovered as a KGB agent who could not be successfully prosecuted because the FBI botched the case. Ronald Pelton, an NSA retiree who was uncovered by NSA—not the FBI—as a result of the Yurchenko defection in the 1980s, was successfully prosecuted largely by good fortune rather than the FBI's skill. Against the NSA's pleadings, the FBI grew tired of watching Pelton and waiting for him to provide court-admissible evidence of his espionage activities. FBI insisted on interviewing him which required that he be reminded of his right to remain silent. Pelton chose instead to admit to his spying activities and tried to convince the FBI to use him as a double agent against the KGB. The FBI's notorious handling the Wen Ho Lee case at the Los Alamos Laboratories is, of course, yet another example of its incompetence at CI. The list could go on.

In a word, the FBI's performance in the 1980s and 1990s is not marked by a *decline* in effectiveness. Rather, poor performance is *normal* over the past half century. The CI performance of the military services and CIA may be no more impressive. They certainly deserve fundamental review and reform. President Clinton's decision directive (PDD-75) on CI, creating layers of interagency boards, committees, and special officials, might be mistaken as such a reform but in fact it was not.

Of all the structural reforms recommended by this study, those concerning CI are the most urgent. Not only are they essential for dealing with Russian espionage, but also with a growing number of hostile intelligence services of other countries. And the prospects for uncovering terrorist networks in the United States will remain dim until US CI capabilities are radically restructured and improved.

The National Reconnaissance Office. Before this study's publication, the NRO was publicly rebuked by the Congress for its loose fiscal controls and other problems. A congressional commission reviewed NRO but failed to call for the kind of structural change essential for ameliorating, if not eliminating them. Most of the problems of NRO result from its status as an independent agency with its own budget which it defends in Congress, supported strongly by its own industrial lobby. In light of this study's analysis in 1997, these problems should have been expected. Its recommendations (see pp. 74 and 82) that the NRO be divided into two parts, one subordinated to NSA, the other to NIMA, remain valid today for procurement of SIGINT and IMINT space-based collection systems as well as for TENCAP programs.

Where the NRO is involved in R&D and procurement of other collection systems, the study was silent, and it remains silent in this reprinting for the lack of a full understanding of all the issues as they now stand. In the area of unmanned aerial surveillance vehicles (e.g., the new Predator) and in reconnaissance aircraft (e.g., the U-2 and the SR-71), the study did not offer any guidance on reform. Nor did it examine the (now-defunct) Defense Airborne Reconnaissance Office (DARO, see Figure ES-1) in the Department of Defense, which was also involved in this area.

Defenders of NRO have long and rightly pointed out that had the development and fielding of aircraft like the U-2 and the SR-71 been left to the Air Force, they likely would have never been built. The same is true for unmanned aerial vehicles. The Army began a program in the 1970s which was still floundering the late 1980s and never came to fruition. Here let us note that, if the reporting on the CIA's employment of its Predator system in the war in Afghanistan is true, this is still a problem area. Turf battles between the military services and the CIA allegedly have been serious.

The National Imagery and Mapping Agency. As mentioned above, this study recommended that the NRO program office for the procurement of IMINT systems in space be placed under the fiscal and budgetary control of NIMA. That has not happened. In 2000, a commission was appointed to review NIMA and to strengthen the organization. Yet its report, rendered in 2001, did not call for such change. Why is not clear.

In the absence of convincing arguments against them, therefore, this study's recommendations for NIMA remain valid today. If implemented fully, NIMA might well take over the DARO and NRO program responsibility for aerial surveillance systems and give them the kind of focus and urgency they have always failed to receive from the military services. And because NIMA is within the Department of Defense, the military services' tactical intelligence needs for such systems should be easier to integrate with those of NIMA.

Covert Action. The study recommended that, insofar as covert action involves paramilitary operations, the CIA/DO retain operational control but that it use Special Operations capabilities from the Defense Department (see p. 95.). In light of the turf battles reported between the CIA and the military services in Afghanistan concerning special operations, *this recommendation appears as sound today as it was in 1997.* So too does the principle of putting CIA/DO under the operational control of regional Commanders-in-Chief (CINCs) during hostilities. Perhaps the military services alone can never create adequate positive intelligence support to make covert paramilitary operations effective, especially their initial insertion, their political connections within an area of operations, and similar kinds of needs, but the CIA has consistently used its coordinating authority to prevent their efforts to do so. Thus a CIA lead is essential. Were the CIA

to be transformed from a polyglot technical/ HUMINT/ collection/analysis organization into primarily a HUMINT organization, accountable to the DCI and the Secretary of Defense for support to military operations (and other requirements), it might be induced to perform this role effectively. High quality special operations forces and equipment, however, are unlikely to be developed within the CIA/DO. They will always be relegated to a low priority compared to recruiting well-placed agents. The cultural clash between “conflict-seeking” attitudes required for effective paramilitary operations and the “conflict-avoiding” attitudes required for agent recruitment will always tilt in favor of the latter at the expense of the former.

The study’s recommended division of responsibilities will by no means solve all of the problems that beset cooperation between U.S. military CINCs and the CIA/DO, but it will force a new level of interaction that could improve cooperation.

Intelligence Community Management and PPBS. Resource management within the IC will remain confused and permit a high degree of unaccountability until a more rigorous PPBS system is established. The recommendations on resource management, therefore, remain valid today (See pp. 41-47.). The same is true for managing intelligence production and establishment of production requirements. The study’s recommendations on this issue also remain valid today (See pp. 36-40.). There have been press reports of a so-called Scowcroft intelligence study, but the study is not public and therefore we cannot assess the degree in which it deals with these kinds of management issues or other important reform matters.

Summary. Little in the way of much-needed structural change has happened since this study was first published. Subsequent studies and commissions have either shied away from the structural issues or have ignored them while focusing on mostly policy issues.

Meanwhile, hostile intelligence penetrations of the IC have become its most serious challenge. Financial and management problems also continue to bedevil the IC, including serious organizational decay within NSA and the NRO, insufficient attention to making NIMA effective, and turf battles between the CIA and the Department of Defense on a range of issues, including special operations during the war in Afghanistan and control over NSA and NIMA.

A major reason advanced for the creation of the CIA in 1947 was that it would prevent another intelligence failure like the one at Pearl Harbor in 1941. Curiously, the CIA failed almost at once with the outbreak of the war in Korea, June 1950. On 11 September 2001, it failed to anticipate the attack on the World Trade Center in New York City and on the Pentagon by Osama bin Laden's al-Qaeda operatives. If Pearl Harbor was sufficient to catalyze major structural reforms in US intelligence, then 11 September, where the damage and surprise were vastly greater, should be sufficient to catalyze an equally dramatic restructuring.

This study may not have all the answers for such a restructuring, but its recommendations should provide a sound basis for starting the process.

LTG William E. Odom, USA (ret.)

Preface

Modernizing Intelligence: Structure and Change for the 21st Century makes numerous recommendations for reform. Several of them are far-reaching, certain to provoke strong objections, and unlikely to be implemented soon. The very organizational logic of some of these recommendations, however, will probably prompt their implementation eventually, over the next decade.

The study is also a diagnosis, a critical analysis. It can be useful, therefore, as an educational text on the structure and nature of the IC for Congressional oversight committees. The IC is arcane, and this diagnosis cannot entirely remove that reality, but it tries to make the IC more accessible to readers who are not familiar with its labyrinthine character. These readers might best refer to the Appendix, “A Description of the Intelligence Process, and the Organizations Discussed in this Study,” before delving into the text of the study itself.

The critical tone of the analysis does not mean that its authors think the IC has been a failure. Far from it. U.S. policy makers and military commanders have been so well served by huge advances in intelligence since World War II that many have come to take them for granted. Overall, the IC has been among the most successful parts of the postwar U.S. national security apparatus. Without basic reforms, however, that judgment will not remain valid indefinitely.

The chairman of the study wishes to express his thanks for the abundant expertise and assistance provided by the members of the study’s senior advisory group. A word of thanks is also due to Vice Admiral Al Burkhalter, USN (ret.) and Lieutenant General James Williams, USA (ret.) for reading the study and offering a number of constructive criticisms.

List of Abbreviations

ACS/I	Assistant Chief of Staff/Intelligence
AIA	Air Force Intelligence Agency
ASD/C3I	Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
ASA	Army Security Agency
CA	Covert Action
CCP	Consolidated Cryptologic Program
CI	Counterintelligence
CIA	Central Intelligence Agency
CIC	Counterintelligence Corps
CID	Criminal Investigation Division
CMS	Community Management Staff
CNN	Cable News Network
CNO	Chief of Naval Operations
COMIREX	Committee for Imagery Exploitation
COMSEC	Communications Security
COS	Chief of Station
CSG	Cryptologic Support Group
DARO	Defense Airborne Reconnaissance Office
DCI	Director of Central Intelligence
DCP	Defense Cryptologic Program
DCSINT	Deputy Chief of Staff of the Army for Intelligence
DDCI	Deputy Director of Central Intelligence
DDO	CIA Deputy Director for Operations
DHS	Defense HUMINT Service
DI, CIA/DI	Directorate of Intelligence, CIA
DIA	Defense Intelligence Agency
DirInt	Director of Intelligence (Marine Corps)
DIS	Defense Investigative Service
DMA	Defense Mapping Agency
DNI	Director of Naval Intelligence
DO, CIA/DO	Directorate of Operations, CIA
DoD	Department of Defense

DoE	Department of Energy
ELINT	Electronic Intelligence
EXDIR/ICA	Executive Director for Intelligence Community Affairs
FBI	Federal Bureau of Investigation
FBIS	Foreign Broadcast Information Service
FY	Fiscal Year
G-2	Army Staff Intelligence
GDIP	General Defense Intelligence Program
HUMINT	Human Intelligence
IC	U.S. Intelligence Community
IC/EXCOM	Intelligence Community Executive Committee
ICS	Intelligence Community Staff
IMINT	Imagery Intelligence
INFOSEC	Computer Security
INR	Bureau of Intelligence and Research
INSCOM	Intelligence and Security Command
ISA	Intelligence Support Activity
IW	Information Warfare
J-2	Joint Staff Intelligence
JCS	Joint Chiefs of Staff
JSTARS	Joint Surveillance Target Attack Radar System
JMIP	Joint Military Intelligence Program
MASINT	Measurement and Signature Intelligence
MIB	Military Intelligence Board
NCIS	National Counterintelligence Service
NCS	National Clandestine Service
NFIB	National Foreign Intelligence Board
NFIC	National Foreign Intelligence Council
NFIP	National Foreign Intelligence Program
NIC	National Intelligence Council
NIE	National Intelligence Estimate
NIMA	National Imagery and Mapping Agency
NIMAP	National Imagery and Mapping Program
NIO	National Intelligence Officer
NIS	Naval Investigative Service
NPIC	National Photographic Interpretation Center

NRO	National Reconnaissance Office
NRP	National Reconnaissance Program
NSA	National Security Agency
NSC	National Security Council
NSD	National Security Division
NSG	Naval Security Group
O&M	Operations and Maintenance
OIS	Office of Intelligence Support
OMB	Office of Management and Budget
ONI	Office of Naval Intelligence
OPCON	Operational Control
OSD	Office of the Secretary of Defense
OSI	Office of Special Investigations
OSS	Office of Strategic Services
PA&E	Office of Program Analysis and Evaluation
PPBS	Planning, Programming, Budgeting System
RDT&E	Research, Development, Testing, and Evaluation
RM	Resource Management
RPV	Remotely Piloted Vehicle
SAC	Strategic Air Command
S&T, CIA/S&T	Directorate of Science and Technology, CIA
SIGINT	Signals Intelligence
SCE	Service Cryptologic Element
SLAR	Side-Looking Airborne Radar
SMO	Support to Military Operations
TENCAP	Tactical Exploitation of National Capabilities
TIARA	Tactical Reconnaissance and Related Activities
UAV	Unmanned Aerial Vehicle
USAINSCOM	U.S. Army Intelligence and Security Command
USSOCCOM	U.S. Special Operations Command

Executive Summary

This study differs from other recent intelligence reform efforts in that it deals primarily with structural and management issues, not policy problems. It establishes a set of concepts and principles as “doctrine” for intelligence operations and resource management and then reviews the major components of the Intelligence Community (IC) against this doctrine as a basis for proposing change. Many of the problems besetting the IC have their roots in structural and organizational dysfunctions. Structural reform is thus necessary.

The study uses no classified information, but instead relies on the experience of several former senior incumbents of the IC for their broad-based knowledge of internal IC affairs and their judgment in avoiding improper disclosures. The report’s sections do not pretend to be definitive or comprehensive in elaborating all the IC’s problems. The proposals for reform, like the critical reviews, are based on a “top down” approach, i.e., dealing with the top structural issues, leaving additional, lower-level reform issues to be worked out after the major structural changes are made for the upper echelons of the IC. The advisory group understands that the recommendations would only begin the process of reform, and in some cases should be considered tentative. In all cases, they should be modified or revoked if they prove ineffective.

Why Intelligence Community Reform?

Numerous efforts at reform of the Intelligence Community have taken place, but few have seriously attempted to reform the IC’s organization. Over the last thirty years, the IC has witnessed enormous changes in the way intelligence is gathered and processed, but during this time, with the exception of the recent establishment of the National Imagery and Mapping Agency (NIMA), the IC has not undergone significant structural reform. Dysfunctions, which are costly in terms of wasted resources and poorly-served policymakers and commanders, have developed, making such reforms necessary. Structural reform of the IC can result in the community operating more efficiently, providing more usable intelligence, on a timely basis, for a given allocation of resources. Whether or not it actually does achieve that result, of course, will depend on the competence of the IC leadership. No organizational reform can overcome the absence of effective leadership and management, but dysfunctional organizational structure can neutralize the efforts of the best leaders.

Principles and Concepts for Intelligence Organization, Operations, Management, and Training

The first problem confronting progress in discussions about IC reform is the lack of a commonly understood set of concepts and principles—i.e., “doctrine”—applicable universally within the Intelligence Community. Today, each agency within the IC has its own doctrine or none at all. Until there is an approved and

accepted set of doctrinal concepts, principles, and terms for the IC as a whole, clarity about reform issues will remain elusive.

Section II spells out a preliminary doctrine for the IC composed of two parts. First, basic “intelligence functions” are defined as well as a number of other functions that are related to or partially performed by the IC, yet are not true intelligence functions. Second, “resource management” concepts and terms are explicated. Not only is the promulgation of an IC doctrine essential; an IC schooling system for middle and senior level intelligence officers is also essential to maintain and update its concepts and principles as well as to ensure its continued understanding throughout the IC.

Recommendation

- The DCI should create an IC senior management education system. This system should have as its core curriculum three areas: IC doctrine, resource management, and leadership and staff work.

The DCI Management Structure for the Intelligence Community

The Director of Central Intelligence (DCI) has an organizational framework that, with strengthening, can allow him to exercise more effective leadership of the IC. The DCI’s management functions include 1) collection management, intelligence analysis, production and dissemination; 2) resource management and policy for the IC; and 3) fostering IC coherence and “community.” A number of steps should be taken to improve the DCI’s ability to carry out these functions.

Recommendations

- Make no statutory changes in the DCI’s authority.
- Strengthen the role of the National Intelligence Council (NIC) as the DCI’s instrument for collection management, providing national-level analysis that is not produced by any other analysis agency or section, overseeing analysis and production throughout all IC components, and ensuring that an IC-wide system of all-source data files and materials is kept available to all intelligence analysis units.
- Separate the Directorate of Intelligence (DI) from CIA, greatly reduce its size, and subordinate it to the DCI through the NIC. It will serve as the DCI’s personal analysis arm.
- Restructure the Community Management Staff (CMS) to facilitate the DCI’s exercise of performance evaluation, resource management, and IC policy. Retain its head at the level of lieutenant general/vice admiral or SES civilian grade 6. Create five primary staff sections: Evaluation Management; Resource Management; Science and Technology; Counterintelligence Management; and Security Policy.
- Retain the National Foreign Intelligence Board (NFIB) and the Intelligence Community Executive Committee (IC/EXCOM).
- Require the DCI to conduct a structural review of the IC every five years.

The Defense Department's (DoD's) Intelligence Structure: Review and Recommendations for Reform

The present DoD intelligence structure can be changed at the top levels in a way that would provide a more effective allocation of responsibilities and missions. Military intelligence organizations provide intelligence for two main purposes: support to military operations (SMO), and support for materiel and force development. These two main types of intelligence support should be organizationally separated. Intelligence is provided by organic intelligence units and by the national collection organizations such as the National Security Agency (NSA) and NIMA. The products of the national collection organizations should be accessible to intelligence officers at every level of command.

DoD Counterintelligence (CI) is fragmented and the different organizations share no common doctrine of organization and operations. CI arrangements in the Office of the Secretary of Defense (OSD) have varied over time but have not resulted in effective CI management. Defense intelligence resources are managed in a fragmented, if not chaotic manner.

Recommendations

- Implement all recommendations for the DCI's management structures and those (below) for Signals Intelligence (SIGINT), Human Intelligence (HUMINT), Imagery Intelligence (IMINT), and Counterintelligence (CI).
- Keep the Defense HUMINT Service (DHS) as a single DoD organization under the operational control (OPCON) of the CIA/DO.
- Create an overt HUMINT organization in DoD as a joint activity that coordinates its activities with the national HUMINT manager.
- Put all DIA electronics intelligence (ELINT) collection under NSA. Put its IMINT collection under NIMA.
- Create a DoD CI management center with OPCON, and policy and program management authority over military service CI capabilities.
- Abolish the National Reconnaissance office (NRO) and transfer its program offices to NSA and NIMA.
- Using DIA spaces, create a formal J-2 intelligence organization on the Joint Staff for SMO.
- Make the Director of DIA the coordinating manager of all intelligence support to materiel and force development—both joint and by the services.
- Create a red-blue Net Assessment Center within DIA responsible directly to the Secretary of Defense.

SIGINT

The SIGINT collection discipline is best structured to exploit changing technology and provide support to national level users and to tactical military forces. Service cryptologic elements (SCEs) are centralized under NSA. Tactical SIGINT units are under NSA OPCON; their program budgets are under NSA management. NSA also has its own personnel hiring and training, R&D and procurement programs, and global communications. NSA thus comes close to providing a national manager system for SIGINT. This arrangement has allowed a highly effective system to emerge in which most of the field operations are handled by the SCEs while the more complex tasks of organizing and controlling the system are left to NSA.

The National Reconnaissance Office has the responsibility for procuring and fielding space-based SIGINT collection systems. NRO is largely an R&D and procurement organization. It is analogous to the R&D and procurement commands within the military services. But the NRO has an independent budget which it defends in Congress and executes independently; no other purely procurement agency in either the IC or the military services has this autonomy. All others must let their budgets be integrated within a single military service's budget or within an intelligence agency's budget. NSA, with operational experience with space SIGINT systems, and NRO have frequently disagreed on procurement goals. This structural problem probably accounts for more wastage of financial resources than any other.

Recommendations

- Make the Director of NSA the national manager for SIGINT and for operational control and management of the entire system.
- Place NRO's SIGINT space systems development and procurement program offices under NSA.
- Assign all of NRO's space imaging systems development and procurement to another program office, for IMINT. This office will be placed under NIMA's control.
- Include the budgets for the SIGINT development and procurement program office within NSA's Consolidated Cryptologic Program (CCP).
- Direct the military services and NSA to make greater efforts to coordinate the CCP with the Defense Cryptologic Program in the Joint Military Intelligence Program, and with tactical SIGINT programs in TIARA.
- Direct the DCI to use his CMS Science and Technology Office for an examination of several sensitive core capabilities in NSA.

IMINT

Imagery Intelligence has been organizationally fragmented, particularly until the creation of the National Imagery and Mapping Agency in October 1996. Two early centers of IMINT were Air Force Intelligence and the CIA; the NRO fielded and largely controlled the overhead capabilities. Advances in technology in the 1970s and 1980s made it possible to produce and transmit IMINT in near-real time to military units, but institutional developments allowing exploitation of these capabilities did not take place: there was no organizational locus to operationalize or manage them. Predictably, U.S. IMINT has been judged inadequate. The creation of NIMA is a positive step. It remains to be seen how this organization will function. Certainly its Director needs the authority over R&D and procurement of IMINT collection systems currently held by NRO, as well as OPCON over most IMINT capabilities in the services, analogous to NSA's OPCON over service cryptologic elements.

Recommendations

- Designate the Director of NIMA the national manager for IMINT.
- Place the NRO's IMINT space systems development and procurement program offices under NIMA.
- Assign the primary coordinating and oversight role to NIMA for all military service IMINT programs.
- Direct NIMA to develop a system for exploiting all IMINT collection capabilities to support military operations (or any other operations) in a time-sensitive manner. This will, of course, require working out coordinated targeting and tasking arrangements with IMINT capabilities organic to tactical military units.

HUMINT

The heart of the HUMINT discipline is the clandestine service. As the Directorate of Operations (DO), it was the core of the CIA when it was founded in 1947. The Director of DO has final approval authority over any military clandestine operation. The DO could take the view that military clandestine capabilities are part of the national HUMINT system and become deeply involved in their targeting and exploitation, but has not. DO and DoD also have paramilitary organizations for CA; DoD's appear to be superior. CIA relations with the State Department are policy, rather than structural, issues, but the increasing presence of the FBI abroad raises important structural issues with regard both to the CIA and to the State Department.

HUMINT faces "culture" problems: while deception and misrepresentation are central to gathering HUMINT, these skills are not helpful to organizational management; and, careers are less rewarding to many due to lack of public recognition. Tensions also exist between Counterintelligence and HUMINT. There is also the problem of what to do if a clandestine service suffers a serious penetration by a hostile intelligence service. The public image of having been penetrated will dissuade potential recruits from

talking to case officers, lest they be identified by another undiscovered mole. Many “culture” issues are leadership and management problems, which cannot be solved by structural reforms.

Recommendations

- Restructure CIA, giving it two major components, the national clandestine service (NCS), and a component for handling overt HUMINT. The Director of this restructured organization would be the National Manager for HUMINT, directly responsible to the DCI.
- Retain a residual Science and Technology capability for support to HUMINT.
- Formally establish an OPCON relationship between CIA/DO (NCS) and military clandestine HUMINT elements analogous to NSA’s relationship with the military SCEs.
- Allow the CIA/DO to retain its status as the covert action agency, but make it dependent on the Defense Department’s capabilities for the conduct of any paramilitary covert actions.
- Take a broad approach to designing and implementing CIA/DO management of overt HUMINT.
- Address CIA/DO “culture” and related problems with a wide range of management, leadership, and organizational reforms, including consideration of disbanding the DO and creating an entirely new clandestine service.

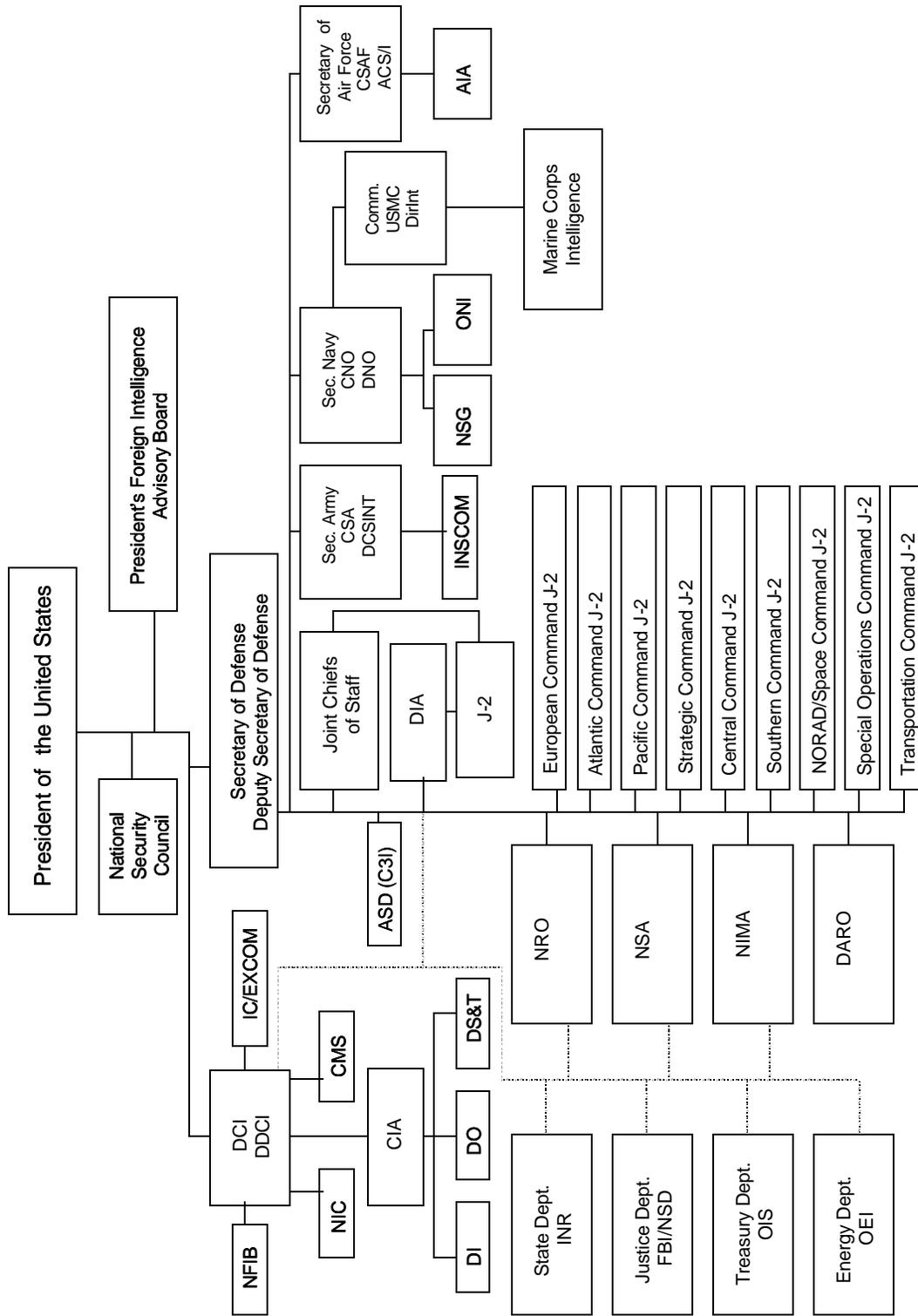
Counterintelligence

The two Counterintelligence problems amenable to structural reforms are the mixing of CI with law enforcement and the mixing of CI with offensive clandestine HUMINT. In DoD, the Navy and the Air Force can create independent CI units on the model of the Army’s “pure” CI structure. Bureaucratic resistance to the transfer of CI from the Federal Bureau of Investigation (FBI) would be monumental, but, assuming that it could be overcome, a preferable arrangement would be a CI national manager, with an independent organization—a national counterintelligence service (NCIS)—and some degree of OPCON over all other CI, including military and CIA. The national manager would disseminate CI for all civilian and military organizations to support their security operations. Having a national CI manager would help ensure the IC’s awareness of hostile efforts to counter it. Effective OPCON and CI support procedures will be necessary if the advantages of a national CI organization are to be realized.

In establishing a national CI service, consideration for protection of the rights of U.S. citizens will be critical. Particular care will be required to identify and apply the legal rules appropriate to CI activities depending on foreign or domestic location and the legal rights of subjects under investigation. Structural changes in CI should not be a means of avoiding legal norms and requirements as they currently exist.

Recommendations

- Create a National Counterintelligence Service (NCIS). The FBI's CI department can form its core, augmented with small elements from CIA's CI organization.
- Designate the Director of the NCIS the national manager for CI, responsible to the DCI in the same way as the national manager for HUMINT.
- Give NCIS coordinating authority over all CI operations within IC components.
- Give the national manager for CI responsibility for providing CI support to all departments and agencies at the national level; experimentation with the national manager assuring CI support to tactical military units should take place.
- Make the national manager for CI responsible to the DCI for maintaining a comprehensive CI picture of all relevant CI target intelligence services.
- Direct the national manager for CI to create a CI school and ensure that it has available the record of all CI cases as its primary instructional material.
- Retain a significant organic CI capability and effort in the CIA/DO and the military services, giving the national manager for CI access to these activities for coordination purposes.



..... Dotted line denotes budgetary programming relationship.

Figure ES-1. The Current U.S. Intelligence Community

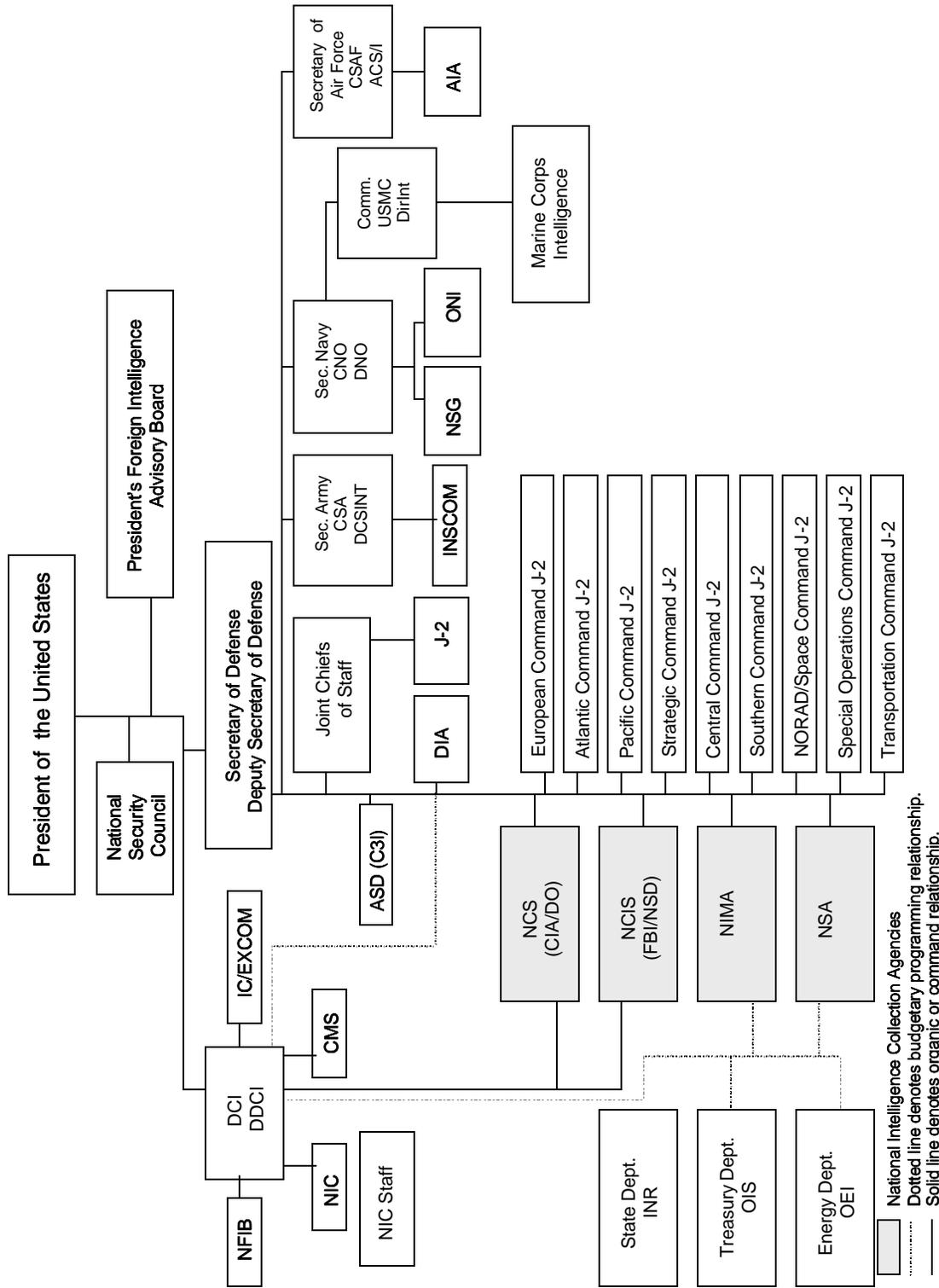


Figure ES-2. The U.S. Intelligence Community, Showing Proposed Organizational Reforms

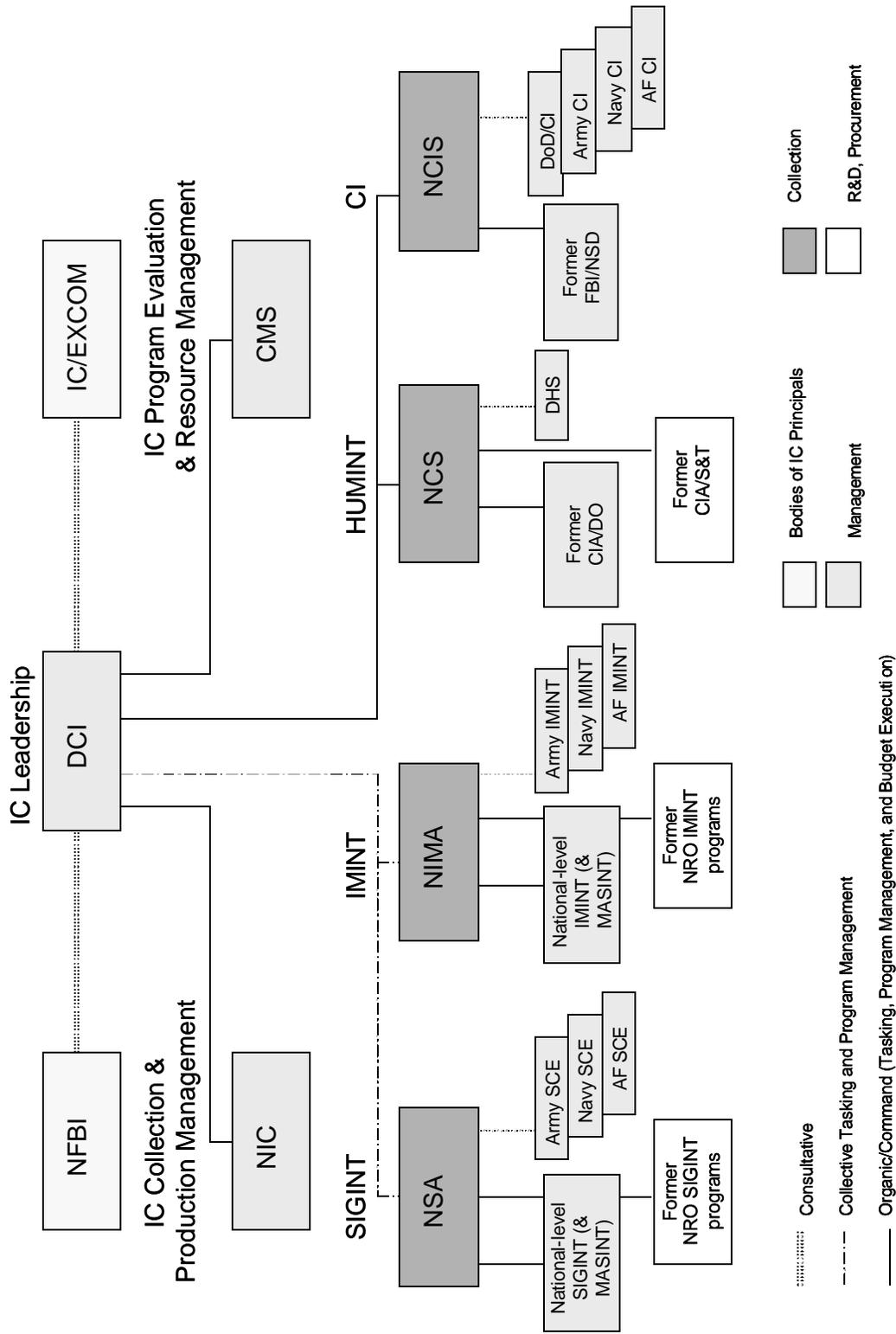


Figure ES-3. Management and Collection Elements of a Reformed U.S. Intelligence Community Arranged by Function

Section I

Introduction: Why Intelligence Community Reform?

Over the last couple of years, studies on intelligence reform have become a cottage industry. Why is another one needed? The answer is simple: most of them have attempted to doctor the symptoms, not the illness. The skeptical reader will object that this claim is not self-evident. At first glance, that may seem a fair reaction, but on deeper examination, it does not stand up to scrutiny. Consider the public record.

Since the Church and Pike committees in the Congress began investigating the Intelligence Community (IC) in the mid-1970s, the issue of intelligence reform has been raised repeatedly. During the Carter Administration, several initiatives were taken to implement some of the ideas produced by the Church committee, but no fundamental structural change occurred. Several times in the 1980s the Congressional oversight committees raised the reform issue, and then-Senator David Boren (D-OK) actually drafted legislation for several structural changes in the IC. The House committee then offered an alternative draft, but neither bill became law. In 1994, Senator John Warner (R-VA) introduced legislation for a presidential commission to consider Intelligence Community reforms, and his bill became law. The resulting commission produced its report in early 1996 [1]. At the same time, several unofficial intelligence reform studies and reports were undertaken, producing a flurry of activity and a wide variety of proposals [2].

Most of these reform efforts were inspired by sensational problems and episodes within the Intelligence Community, especially in the Central Intelligence Agency (CIA). The Church committee was outraged by evidence that CIA had actually attempted assassinations as part of covert actions in the past, and that the Army's counterintelligence units had been used to help the FBI keep track of anti-war movement leaders in the late 1960s and early 1970s. In the late 1980s, CIA covert actions in Central America and related activities by National Security Council (NSC) staff members became the focus of renewed interest in intelligence reform. In the 1990s, a number of incidents within the CIA, some having to do with personnel policies, others involving serious operational failures, and still others involving National Reconnaissance Office (NRO) accountability for funds, brought the issue once again to Congressional and public attention. The discovery that Aldrich Ames of CIA's Directorate of Operations (DO) was a KGB agent produced a new and unprecedented level of concern.

After two decades of such episodes, no fundamental reform has occurred. Virtually all Congressional investigations and reform studies have merely focused on the scandals and raised policy issues. For example, should the CIA be permitted to carry out assassinations? Should Army Counterintelligence (CI) be involved in domestic surveillance of civilians? Should CIA clandestine officers be allowed to have cover as journalists? Should the Intelligence Community budget be made public? And so on.

Almost none of the Congressional committees' efforts at reform have addressed structural, organizational, and management issues. The major exception was Senator Boren's draft legislation which directed the creation of a national imagery agency and a few other organizational changes. A second partial exception

has been *IC21*, the House Permanent Select Committee on Intelligence's recent organizational redesign proposal [β]. The recent presidential commission, of course, was instructed to examine the roles and missions of all the parts of the Intelligence Community—an invitation to deal with the structural issues—but it effectively declined the invitation.

Recently, however, one major feature in Boren bill in the late 1980s, the creation of a national imagery agency, has actually been accepted with the formation of the National Imagery and Mapping Agency (NIMA) on 1 October 1996. A few additional but minor organizational steps have been taken in connection with the old Intelligence Community Staff (ICS), now reorganized and renamed as the Community Management Staff (CMS). Immediately after the Ames case broke, a flurry of activity centered on the traditional FBI/CIA dispute over counterintelligence turf, but interest soon abated.

With the exception of the creation of NIMA, however, structural reform has been largely ignored. This is both strange and unfortunate. Several senators and House members proved highly reluctant to delve into the structural issues. The CIA and most Directors of Central Intelligence (DCIs) have also resisted serious review of the structural problems. Thus a quiet and informal consensus that nothing structurally is wrong has prevailed, not only in Congress and the Intelligence Community itself but also in the presidential commission as well. Private sector intelligence reform studies have followed suit.

The reasons why are not entirely clear, especially after Senator Boren opened the question of deeper problems in need of structural solutions. Senator Dennis DeConcini (D-AZ) complained about the "culture" at CIA as the problem. Organizational cultures are normally the products of structural conditions. The accumulating incidents should have made both administration officials and the Congressional committees suspect that they were looking at the symptoms, not really the ills.

Are there really serious structural and organizational problems? One does not need access to classified information to answer yes. It would be extraordinarily surprising if there were not. The repeated incidents that upset the Congressional oversight committees must be symptomatic of larger problems. That Aldrich Ames could be recruited by the KGB, meet KGB case officers undetected for years, and make "dead drops" in Washington DC under the nose of the FBI suggests that more than policy problems are involved. That General Schwarzkopf, who probably had better intelligence support than any commander in history, would complain bitterly about problems with intelligence (primarily imagery intelligence) indicates that more than policy problems beset the Intelligence Community. That the National Reconnaissance Office (NRO) could have very large sums of money and spend them on facilities without the Congressional committees' knowledge indicates deeper problems. Not so well known to the public but widely known in military circles, lack of CIA human intelligence support to military operations in the failed attempt to rescue hostages in Iran, lack of similar support in the Persian Gulf War and on other occasions, and serious bureaucratic turf fights between NRO and other agencies, are more evidence of deeper problems. Incumbents come and go, but the structural arrangements and the resulting problems have remained constant or worsened.

Another way to infer that structural problems are serious is to recall that, after the Intelligence Community structure had settled into place—a time span of more than three decades—no major changes have occurred. At the same time, the introduction of new leading-edge technologies has occurred at a rapid pace over those

decades. In the 1960s, transoceanic communications were fairly limited. That fact required a significant number of technical intelligence activities to be located in Europe and East Asia. A decade later, many of them had been moved to the United States. The new and large space-based communication capabilities made possible radically different and more effective ways of gathering, processing and producing, and distributing intelligence. The communications revolution alone provides grounds for suspecting that major structural reforms in the Intelligence Community are long overdue. Some adaptations have been made, but by no means all that the technologies require for their full exploitation.

The introduction of intelligence collection systems in space created radically new possibilities, and many of them were exploited. As time passed, however, and as the number and variety of space systems increased, new ways to exploit them became possible that could not have been foreseen in the 1960s. Most such opportunities, however, require organizational changes, and very few were made. A national imagery agency, for example, should have been created fifteen or twenty years ago to exploit new technology, but bureaucratic turf concerns kept the very idea from being considered. Even NIMA's creation in 1996 does not assure that it will be given all the authority required to make the most of imaging systems.

Another indication of structural problems is found in the continuing debate between CIA and the Defense Intelligence Agency (DIA) on estimates of Soviet military capabilities throughout the Cold War. The gross underestimate of Soviet military expenditures can be explained largely as the result of competition between these agencies which caused each to be less concerned with the truth of matters in the Soviet Union and more concerned with proving the other wrong in the eyes of the Congress. The needs of Executive Branch policy makers, for whom this intelligence was primarily produced, tended to be secondary in both agencies' calculations. The FBI's jealousy over its counterintelligence turf, not only vis-a-vis the CIA but also vis-a-vis the military services' counterintelligence operations, is a similar symptom of structural problems.

These two examples suggest that structural problems distorted U.S. perceptions of Soviet military and economic capabilities and permitted the KGB to penetrate our own intelligence services to a degree that was preventable.

Failure to make appropriate organizational changes to exploit evolving technology also caused financial inefficiencies. The costs of technical intelligence collection systems dwarf the costs of intelligence analysis and clandestine human intelligence operations. Yet efficiency in the purchase of technical systems has hardly been considered. In the 1950s and 1960s, this was more understandable, as there was not yet adequate experience with most new technologies to allow meaningful efficiency comparisons. In some cases it could also be argued that Intelligence Community technologies more than paid for themselves as they migrated into the civilian economy. For example, development of modern digital computational means (i.e., computers) occurred almost entirely as a result of the National Security Agency's R&D efforts in the 1950s. IBM and CDC essentially got their start in modern computers from NSA funding, and without it, we might be two decades behind where we are in computers today.

In the 1970s and '80s, however, these arguments for ignoring the burgeoning costs of technical collection programs lost their cogency. Bureaucratic processes and organizational interests, however, stood in the way of examining costs and reducing them. Predictably, inefficiencies mounted. Covered by secrecy, arcane organizational practices, and technical complexities, these accumulating structural-management issues

have remained largely opaque to the Congressional oversight committees and also to high level officials in the Executive Branch. Neither DCIs nor Secretaries of Defense have really understood them fully.

None of the accumulating inefficiencies and missed opportunities for better and more efficient exploitation should be terribly surprising in organizations dealing with fairly rapid change in leading-edge technologies. No one would expect IBM, AT&T, GMC, Chrysler, or other large industrial firms to make no fundamental structural changes for three decades. All of these firms were slow to make changes, but they did make them, in the face of serious financial difficulties resulting from business competition. Management at all levels in organizations tends to resist change, especially structural reforms. If change is necessary for these large business organizations, is it not also true for the Intelligence Community? In fact, it is.

In light of all these points, another critical study of the Intelligence Community is surely justified, but not just any additional study. There is surely a strong case for a review of the IC's structure, organization, and management arrangements. And indeed, that is the focus of this study.

This study is *not* concerned with issues that brought media attention to the Council on Foreign Relations intelligence study: whether or not CIA should put agents under cover as journalists. It is not concerned with whether or not the CIA predicted the collapse of the Soviet Union. It is not concerned with proper security rules and techniques for preventing another "Ames" case. It is not concerned with whether more intelligence attention should be put on the Third World, terrorism, nuclear proliferation, Russia, or economic affairs. Nor is it concerned with whether or not the United States should engage in covert actions, or whether or not the United States should have an intelligence community. These are issues treated in most other studies, and all of them are policy problems. They are important, but they are different from management and structural problems. Thus they will be treated here only when they appear as symptoms of structural problems.

To clarify this distinction with a metaphor, assume that the Intelligence Community is a ship which has had numerous problems on its recent voyages. It is now in harbor for repairs. Most of the previous reform studies ask where it should sail next, when it should sail, what flag it should fly, what color to paint the ship, etc. Here those questions will be set aside and primary attention focused on the ship's hull, its engines, its navigation gear, etc., looking for malfunctions and prescribing needed repairs. When the repairs are completed, it can then sail anywhere, any time, and under any flag with any passengers. These choices are up to Executive Branch policy-makers and military officials served by the Intelligence Community.

Some Points About the Study's Methods

No classified information is used in the study. Most of the information about structure and organization of the Intelligence Community is public, and that is the most important information for this effort.

At the same time, those directing and advising the effort include mainly people with lengthy experience in the Intelligence Community at fairly high levels. Their backgrounds and experience are a substitute for the inside look that the presidential commission's study enjoyed. In some instances, this experience is

somewhat dated, and where the Intelligence Community has already made changes that are recommended, so much the better. One example, already apparent, is the creation of the National Imagery and Mapping Agency, which was founded several months after this study began. Still, virtually all recommendations are relevant to the IC, even for offices that have undergone some reorganization. Periodic rearrangement of the deck chairs on the ship "Intelligence Community" has occurred from time to time with little or no impact on the basic structure and processes.

The study begins with an elaboration of principles and concepts for intelligence. Its purpose is to provide a conceptual reference against which to assess the appropriateness of both the present Intelligence Community structure and recommended reforms. It is also an important basis for common definitions and terms, an intelligence vocabulary which has been lacking in the Intelligence Community and has been the source of a great deal of misunderstanding and misleading debate. Serious critics who basically disagree with the study will, therefore, offer a different set of concepts and principles. Only thus can a meaningful dialogue on reform take place.

The succeeding parts of the study deal with management structures, intelligence collection disciplines, linkages to users of intelligence, and processes required to make the system work effectively in light of new technologies and various users' needs and operational circumstances.

None of the separate study parts pretends to be definitive in elaborating all the problems. Classification and security concerns make that impossible. So do resources for the study, which are quite modest. Instead, each part is descriptive of major and reasonably well known problems, offering selected illustrations to clarify them. The recommendations at the end of each part follow from the analysis and should be consistent with the "principles and concepts" paper on doctrine.

In many cases, the recommendations, if enacted, would only begin a process of reform. Much additional change would have to follow, based on experience and results.

In some cases, recommendations are tentative because the authors and the advisory group are either not fully agreed or not entirely certain in their minds and experience that they are the best solutions. These recommendations do, however, respond to real problems, even if they may not be optimally effective responses.

Several issues cut across several parts of the overall study. That imposes some repetition, but it also helps provide integration to the entire set of recommendations.

Finally, a number of positive organizational trends are identified and emphasized for continuation and completion. Among the most important is the trend toward providing the DCI with effective structures and processes to manage the entire Intelligence Community. A consolidated Intelligence Community program budget, the Community Management Staff, and a few other developments mark the general trend over a couple of decades for the DCI to make the management of the Intelligence Community his main rather than his secondary responsibility. There are other examples, e.g., the consolidation of a single collection discipline under a "national manager," a trend in signals intelligence that has yet to reach completion but which has progressed farther there than in other collection disciplines.

Readers who are not generally familiar with the structure of the Intelligence Community may want to review the Appendix, which provides a description. The reader may choose to do so at once, or may proceed directly with the report and refer to the Appendix according to his need for organizational clarification. While IC organizational charts are found in the Appendix, considerable textual description is also provided in order to orient the uninitiated into the IC's complex structure and interagency character.

Notes

1. Presidential Commission on the Roles and Capabilities of the United States Intelligence Community (hereinafter the Aspin-Brown Commission), *Preparing for the 21st Century: An Appraisal of U.S. Intelligence* (Washington: GPO, 1996, 151 pp., plus appendices).

2. See *Making Intelligence Smarter: The Future of U.S. Intelligence*. (New York: Council on Foreign Relations, 1996, 39 pp.); *The Future of U.S. Intelligence* (Washington: Consortium for the Study of Intelligence, 1996, 82 pp.); *In From the Cold: The Report of the Twentieth Century Fund Task Force on the Future of U.S. Intelligence* (New York: Twentieth Century Fund Press, 1996, 275 pp.).

3. *IC21: Intelligence Community in the 21st Century*. Staff Study, House Permanent Select Committee on Intelligence (Washington: USGPO, 1996), 330 pp. plus appendices. See also *IC21: The Intelligence Community in the 21st Century, Hearings of the House Permanent Select Committee on Intelligence*, May 22-December 19, 1995 (Washington: USGPO, 1996, 393 pp.).

The Congress as part (Title VIII) of the FY1997 Intelligence Authorization Act (Public Law 104-293—Oct. 11, 1996) passed the Intelligence Renewal and Reform Act of 1996 (50 USC 401 note). Some of its provisions reflect the recommendations of IC21. The Act created some new offices in the "Office of the Director of Central Intelligence," and formalized some informal authorities of the DCI. The Act did not, however, change the basic structure of the IC, so its changes, while probably beneficial, must be regarded as largely cosmetic.

Section II

Principles and Concepts for Intelligence Organization, Operations, Management, and Training

Introduction

The major problem confronting all discussions about reform of the U.S. Intelligence Community is the absence of a commonly understood and accepted doctrine for intelligence organization, operations, and management. Virtually every agency within the IC has either a unique doctrine or no doctrine at all. The Director of Central Intelligence has never promulgated such a set of principles and concepts. Some vague ideas about the topic have been generally present in the Community Management Staff, but these ideas were never fully developed, or promulgated as official guidance. The Central Intelligence Agency, the National Security Agency, and the Defense Intelligence Agency have internal standard procedures but not what could be called a clearly articulated doctrine. The compatibility among their inchoate or de facto standard procedures is far from complete. The intelligence staff (J-2) structure within the military's joint system of unified and specified commands is without a doctrine although a few standard concepts tend to prevail in several of the J-2 staff sections. The military services vary in their conceptions of the intelligence process and functions. The Army has the most rigorously articulated intelligence doctrine; the Navy's practice is fairly well standardized but not as formal as the Army's; and the Air Force tends to have practices that differ significantly among major commands. Even less articulation of standard practices for their intelligence components (very small, mostly analysis staffs) is found within the civilian cabinet departments and agencies.

Between the early 1950s, when the Intelligence Community was beginning its development, and the 1990s, vast technological change occurred in collection systems and communications. The use of space-based systems radically altered collection operations. The evolution of global communications networks with vast bandwidth for transmission brought a structural revolution in many aspects of military intelligence as well as intelligence support to diplomacy.

For example, most of the order-of-battle intelligence on Soviet forces in Eastern Europe was developed and maintained within the European Command as late as the mid-1960s. Space-based collection and transoceanic high-speed communications soon thereafter allowed this activity to be centralized in various agencies in Washington, D.C. These changes occurred with little concern for maintenance of a systemic doctrine that could foster a common understanding of their rationales and how they would be adapted to crisis operations and war time. Accordingly, U.S. forces in Europe were not always the beneficiaries of the centralization process. Parochial bureaucratic battles followed. Some commands in Europe, especially the Army component, felt cut off, deprived by what it perceived as the "national systems" taking over and leaving them out in the cold. Many Air Force units had a similar reaction. As a result, Army and Air Force commands tried to develop independent approaches, especially for wartime operations, because they either

did not realize that national systems could be made to support tactical operations in Europe or they did not trust that such systems would give them priority support in an emergency.

At the national level within the Intelligence Community, little genuine effort was made to rectify the situation in Europe, or in the Pacific Theater where similar changes occurred. In part this was due to primary concern with the intelligence user community in Washington, but it was also due to simple ignorance at the national level about both the needs of military forces and of the ways that communications could be developed to meet them. Much lip service to “support for military operations” was given, but little of note was done until the early 1980s, and even here it was done on an ad hoc basis almost entirely by NSA and DIA.

Within the Washington Intelligence Community, numerous efforts were made by the DCI’s Intelligence Community Staff, now the Community Management Staff, to come to grips with these problems. It actually created a system for formal intelligence requirements and tried to tie resource allocations to meet them. Still, progress was slow, and bureaucratic struggles were intense.

In the 1980s, the DCI’s Intelligence Community Executive Committee (IC/EXCOM), which then was called the National Foreign Intelligence Council (NFIC), attempted repeatedly to relate budgets to various parts of intelligence activities according to perceived user demands. Almost none of the members of the NFIC, however, possessed the means to assess the connection between resource inputs and intelligence outputs in ways that would allow the DCI to make effective program decisions in cutting, shifting, or increasing resources. The NFIC membership included the heads of all the major intelligence activities rather than a set of people who had a working knowledge of these input-output connections. In most cases, *such people did not exist*, because the IC had grown up without such a resource-management doctrine as a guide.

The arcane and compartmented character of most intelligence activities also contributed to a lack of understanding of the problems confronting the IC. Senior officials most often spend careers in a single agency, and therefore, they arrive in senior posts largely ignorant of other parts of the IC. Without a set of principles—that is, a doctrine—for intelligence operations and management, they have behaved as any organization theorist would predict: they have defended the parochial resource interests of their home agencies. This kind of behavior has consistently reinforced the national-tactical split in the IC, and it has produced long-standing fragmentation among the national-level agencies. This is not to say that the IC has made no progress; rather it is to point out that over time it accumulated many structural obstacles and inefficiencies that increasingly slowed progress. Lacking any clear principles for judging the effectiveness and rationality of changes, it could not be otherwise.

Until a set of principles and concepts is specified and made official doctrine, this dysfunctional behavior will continue. Within the IC, a tower of babble long ago replaced a language of mutual understanding. Only occasional crises, usually military conflicts, forced a degree of improvisation that overcame the more conspicuous dysfunctions, but often such improvement has been temporary.

The remainder of this section, therefore, spells out an IC doctrine. It need not be the last word, but it will serve as the starting point and the guidance for all of the analyses and resulting recommendations of this study. It draws on two sources for concepts and principles of intelligence operations.

First, it takes the Army's basic pattern emerging from World War II and in the immediate postwar decades. The Navy and the Air Force patterns are too specialized and particularized to serve as a general model, although their intelligence operations can be adapted and understood in the context of the Army's doctrine. Their operations are heavily based on a few large weapons systems while the Army's operations are far more diverse and complex, demanding a more generalized approach.

Second, because intelligence operations have much in common with the operations of news operations—the press and television—and because they have adapted to modern technology, they provide another model from which certain principles can be drawn.

For management of resources, the models from which principles are taken here include general organization theory, business firms, and non-profit organizations. Business principles alone are not adequate because the IC does not sell its products in a competitive market. Thus the non-profit case must also be included, not just private sector organizations but also public agencies, in particular the Defense Department which has adapted the Planning, Program, Budgeting System for managing resources.

Specification of Functions

Intelligence operations can be divided into a finite set of functions. The ones listed here are not innovations, but rather longstanding and generally accepted throughout the IC. They are a) collection management, b) collection, c) analysis and production, and d) dissemination. Intelligence operations, like news operations, have a cycle which is shown in Figure 1. It starts with collection management. The collection manager must determine what intelligence is needed, just as editors decide what issues to cover with reporting. Next the collection manager must issue directions to collectors, telling them what information is needed, just as editors dispatch reporters to get stories. The collectors report back to the collection manager who then gives the information to analysts. Analysts develop that information—analyze it—into intelligence products. In news agencies, this is the editorial part of the cycle. The products must then be disseminated to the user who stated the initial requirement, starting the cycle. And they must be disseminated to any other user who needs them even if he did not request them. The users provide feedback to the collection manager. This process, of course, is analogous to the printing and publication of newspapers or magazine TV and radio scripting and broadcast.

A number of other activities might come to mind which are not included in these intelligence functions. They need to be identified and their omission explained.

Security is often considered an intelligence function by the IC. The DCI has some security policy responsibilities, but implementation of security is not an intelligence function. It is a “command” function (or “management” function in civil agencies). The Secretary of Defense, unified commanders, and service chiefs are directly responsible for security. So is the Secretary of State and the heads of other departments and agencies. The intelligence staff officers in these departments cannot manage security because they lack the authority to issue directives and orders required for maintaining security. Security is an “operations” function just like a battle plan or organization policy. In fact, operations plans normally have a security

operations portion. Heads of intelligence organizations are responsible for the security of those organizations precisely because they do have full directive authority over them.

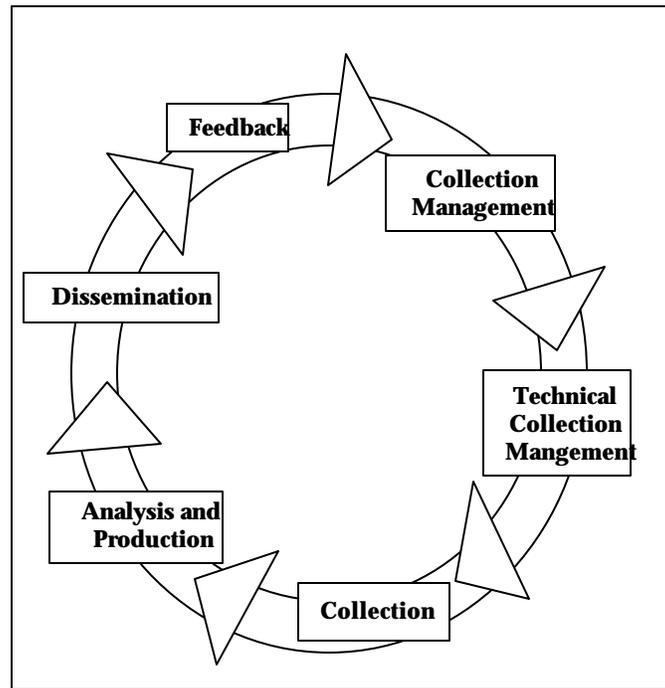


Figure 1. The Intelligence Cycle

To offer a practical example, Soviet penetrations of the U.S. Embassy in Moscow were not the responsibility of any part of the IC to stop. They were first of all the ambassador's responsibility and finally the Secretary of State's responsibility. The IC's responsibility was to discover them and then to provide technical advice on how the State Department's line management could prevent them.

Counterintelligence (CI) is also sometimes treated as a special function. It is different in some regards, but it is also subsumed in the four primary functions. CI is intelligence about an adversary's intelligence capabilities, targets, means, techniques, etc. It is a subset of intelligence analysis and production, a special kind of intelligence product. Counterintelligence is used by commanders and agency heads to support their security practices, to make them effective. And it is used by law-enforcement agencies to arrest enemy agents and to prosecute them. It is also used by commanders and policy-makers to support "deception" operations and "covert actions." CI has its special features, but so do many other types of intelligence analysis and production.

CI depends on collection directed at the adversary's intelligence capabilities and activities. Collection managers must direct collection toward these targets. The results are used for CI analysis and production.

Covert Action (CA) is not, properly speaking, intelligence. Traditionally, of course, the DCI has directed CA and only the CIA's Directorate of Operations (DO) has carried it out. Yet CA is actually "operations" in the same sense that the aims of foreign policy are implemented by diplomatic operations, and that military objectives are achieved by military operations. Covert Action involves undertaking actions that cannot be

directly attributed to the United States government. CA is meant to influence events without the objects of the influence being aware of the actual source of the influence.

CA is normally divided into two general types, paramilitary and all other CA. The non-paramilitary forms of CA include black propaganda, using agents of influence, and many other means. No force is involved. Rather, political means are the weapons for this type of CA. Paramilitary CA involves training and using paramilitary, and sometimes regular military units for combat operations, most often insurgency operations, to achieve a goal.

CA can be conducted when the United States is at peace or when it is at war. In peacetime, paramilitary CA has always been under the DCI's direction. In wartime, the picture has been muddy. The Defense Department's Special Operations forces are trained for paramilitary CA. In the Korean War, the DCI and the U.S. Army were both involved. The same was true during the Vietnam War and the Persian Gulf conflict. In principle, the DCI is supposed to "chop," i.e., transfer control of, all paramilitary CA to the unified commanders. In practice, it has remained a disputed matter, as was seen most recently during the Persian Gulf War.

Principles for Organizing to Perform Intelligence Functions

Collection management. This function means different things in different places within the IC, but the primary place for it is in the intelligence analysis and production staff sections in all intelligence-using departments, agencies, and military units. That is where intelligence needs are determined, and therefore, it makes sense to put collection management under the command responsibility of the users, actually carried out by the organic intelligence staff sections of the using departments, commands, and agencies. No one else in the IC is in a position to know better what intelligence users need.

Within specialized collection agencies and organizations, a somewhat different "technical collection management" function is required. There, managers must take the collection requirements coming from intelligence-using organizations and translate them into meaning for the collectors. These managers must orchestrate the collectors to best use the wide range of collectors' capabilities and access for satisfying the requirements. In technical collection organizations, this is normally a highly complicated and specialized activity, and it varies radically among collection agencies and capabilities, depending on the technologies involved.

In the military services, and sometimes in civilian departments and agencies, the intelligence staff "general collection" managers are painfully ignorant of the character of "technical collection" management within collection agencies, leading to confusion about who is really giving what collection direction. Clarification of the two types of collection management, therefore, is absolutely essential.

Collection. In modern times, three major and distinct collection disciplines have emerged: human intelligence (HUMINT), signals intelligence (SIGINT); and imagery intelligence (IMINT).

The technical specialization in all three collection disciplines long ago reached a point that required them to be organized separately. No single collection organization can easily manage the training and operation of all three disciplines alone. That organizational differentiation first appeared in clandestine HUMINT, then in SIGINT, and now in IMINT.

HUMINT can be further divided into overt and clandestine collection. The skills and techniques for clandestine HUMINT, of course, are quite different from overt HUMINT, and therefore, organizing for each is equally different. So too is organizing the reporting and distribution of the intelligence collected by each means.

SIGINT began as “communications” intelligence, that is, collecting messages sent by electronic means. As other electronic emanations, e.g., radars, emerged in World War II and later, collection of their signals was undertaken and exploited for intelligence. ELINT (electronic intelligence) became the acronym for this part of SIGINT. The spectrum of signals emanations extends to include visible light, and a number of light signals have emerged more recently that can be collected for intelligence purposes; laser emissions and electro-optics, for example. This area has created management problems about where such collection should be done, by whom, and how to manage it. MASINT (measurement and signature intelligence) is the acronym used to identify some of this kind of intelligence collection. Here we shall only note that ambiguity has arisen about how to draw the organizational boundaries for this kind of intelligence collection.

IMINT began as photography, but in the last few decades, other imaging techniques have been added. Cartography and mapping have come to depend heavily on imaging from intelligence collection systems in space. Thus an argument can be made for lumping military and other mapping within this collection discipline. Technology has already pushed it quite far in that direction.

At the national level, SIGINT has been largely concentrated under the roof of the National Security Agency. Still, some SIGINT, especially ELINT, is highly fragmented organizationally. The trend since the early 1950s, however, has been to increase NSA’s “operational control” (OPCON), as distinct from direct command and organizational ownership, over more and more of SIGINT collection and processing. Each military service has large SIGINT organizations. NSA does not command them, but it exercises OPCON over these military “service cryptologic elements” (SCEs). Lower level tactical SIGINT capabilities remain under military service OPCON as well as command in some cases, not a very satisfactory situation for effective collection. This OPCON turf boundary has always been a major dispute between NSA and the military services. Where military commanders have a good technical understanding of SIGINT, the dispute generally fades, but that understanding is far from uniform.

The SIGINT model of distinguishing organic ownership (command) of collection organizations from operational control (OPCON), must be kept in mind as an effective approach for cross-agency and cross-organization management of collection operations. It is the only way orchestration of IMINT collection can successfully be brought under a single national-level management structure. And it probably offers solutions to the traditional problems of coordinating CIA’s clandestine and overt HUMINT with Defense Department HUMINT.

At the national level, clandestine HUMINT has long been centralized in the Directorate of Operations in the Central Intelligence Agency. Fairly large clandestine HUMINT capabilities have existed within the Defense Department, but its operations are at the coordinating discretion of the CIA/DO. In principle, the CIA/DO has the same kind of OPCON over military clandestine HUMINT as NSA has over the SCEs, but the sociology of HUMINT organizations has made it difficult to achieve the kind of cooperation between military and CIA/DO HUMINT that exists between NSA and the SCEs. The NSA-SCE model, however, has a lot to offer the national-level management of clandestine HUMINT.

Overt HUMINT is carried out by a plethora of agencies and organizations, many with no IC affiliation. Debriefings of defectors, travelers, and many other potential sources clearly belong within the IC. Collection of information from foreign news media, now done by the Federal Broadcast Information System (FBIS), is in the IC. The defense attaché system, another overt HUMINT collector, is within the Defense Intelligence Agency. Prisoner of war (POW) interrogation units, yet another overt HUMINT collector, are found within the military services. Diplomatic reports, subscriptions to foreign publications and book purchases, information gleaned from meetings between U.S. and foreign officials, and several other kinds of overt HUMINT are outside the IC. The degree of exploitation of these overt sources varies widely and is normally low. The whole of the overt HUMINT collection discipline lacks a coherent management structure.

The organizational principle advocated here, of course, is a system of “national managers” for each of the three collection disciplines. Until the Central Imagery Office was formed in 1992, IMINT lacked any semblance of a managing office. The Community Management Staff previously tried to manage IMINT through one of its committees. As communications and IMINT technology have changed, this committee structure proved increasingly ineffective. Even the creation of NIMA in 1996 has not completely clarified the operation of IMINT assets. Overt HUMINT has been almost as poorly managed, but because the public media, especially TV, have become increasingly important, the deficiencies in overt HUMINT management are not felt so acutely. The news media compensate enormously.

Analysis and production. This function is best performed close to the users of the intelligence product, normally by intelligence staff sections in the user organization. Using their collection management function, they can draw on the collection agencies to provide raw or processed intelligence for analysis, tailoring their products precisely for the users’ needs. Alternatively, or additionally, it can be performed at centralized or separate analysis centers, apart from the intelligence staff sections of user military organizations and their equivalents in civilian agencies. To use an analogy from modern computer systems, a “distributed processing” is the first model, and “central processing” is the second model. Large central “processing” (analysis and production) centers have greater capacities, but they tend to be less responsive to precise user needs. The two approaches can be mixed by augmenting the “distributed” intelligence staff sections with separate supporting analysis and production units. For some types of analysis and production, large national centers may make sense, but the principle of “distributed” intelligence analysis and production is obviously preferable because it is better located to be attuned and responsive to users’ needs.

Dissemination. This function, of course, involves getting usable intelligence products to the appropriate users. It concerns the collection organizations’ distribution in response to collection managers, and

includes timely distribution from analysis and production staff sections to their coordinate using staff sections as well as to lower units.

Dissemination is at root a communications issue. It includes the personal interaction between intelligence staffs and their users. And of course it includes the electronic or any other message system between collectors and producers, between producers and users, and sometimes directly between collectors and users when a single-source collection can be used without additional analysis or processing.

Command and management principles in military organizations sometimes interfere with rapid dissemination of intelligence. When intelligence derived at the national level through HUMINT, IMINT, or SIGINT collection is needed and usable at the tactical level in a unified command, it may be delayed in reaching a needy user by higher intelligence staff echelons as it passes downward. With modern communications and with the rapidity of operations at the tactical level, direct dissemination is often the best solution.

This aspect of dissemination is also related to the question of “dedicated” intelligence communications nets, something military communications experts tend to oppose. Considerable progress has been made in overcoming the conflicts between mutually exclusive principles for intelligence dissemination, but it remains a dynamic and challenging problem.

Counterintelligence. Although CI is not, properly speaking, an independent intelligence function, it has uniqueness that requires treatment as an independent function.

First, CI involves operations within the United States and within the ranks of the military services and civilian departments. Thus it straddles the foreign and domestic boundary. For collection targets it must look within the very ranks of the IC.

Second, it may lead to indictments and prosecution in courts of law. That involves it with the U.S. judicial system in a way that no other part of the IC is fully involved.

Third, its targets may include U.S. citizens who have no formal government affiliation.

Fourth, while military commanders and civilian department heads use CI products to support their “security” operations and practices, CI is also used for CI operations and clandestine HUMINT operations. Double agents are an example.

All of these characteristics of CI argue for a management organization with a considerable degree of autonomy. At the national level, an overall picture is essential if the CI effort is to avoid leaving large openings and vulnerabilities for hostile intelligence operations to exploit. The first principle, therefore, is that a national-level manager, having OPCON over CI within all departments and agencies, is essential.

A second principle concerns CI’s connection to law enforcement. Because espionage against the United States is a crime, CI leads to law enforcement operations. At the same time, catching spies and uncovering foreign technical collection capabilities within the United States (as well as abroad) are activities more complicated than catching domestic and foreign criminals. The motivations and resources backing

criminals are different from those backing foreign intelligence services. Criminal investigation skills, therefore, often work very poorly in CI operations. CI and law enforcement are mixed organizationally in the Federal Bureau of Investigation, in the Air Force's Office of Special Investigations (OSI), and in the Navy's Naval Investigative Service (NIS). Only in the Army, where the Criminal Investigation Division (CID) and CI units are separate, is CI clearly differentiated from law enforcement in an organizational sense. The CIA's CI operations are entangled with its offensive HUMINT, another mix of operations that has drawbacks. Strong arguments for mixing offensive HUMINT and CI in a single organization in some cases can be made, but the arguments for mixing CI and law enforcement against ordinary criminals are not compelling. This set of issues needs effective examination.

A multi-disciplinary approach to CI. A third principle for CI concerns its support by collectors. CI organizations quite naturally want to run their own clandestine HUMINT, e.g., double agents and penetrations. This is commonly understood. CI exploitation of SIGINT collection improved in the 1980s, but it can still make progress. Use of IMINT for the entire array of imagery collection has not made the same progress. A "multi-disciplinary" approach to collection for CI is an imperative principle in today's world of changing technology.

Covert action (CA). The overall utility of CA has been a hotly disputed issue. Here we will set it aside and assume that the U.S. government will want to retain at least some capabilities for CA.

Non-military CA probably has no other logical organizational disposition except within the clandestine HUMINT organization. Legally, however, the boundary between HUMINT and CA has to be kept extremely clear. Influencing a foreign government without letting it know the source is a tricky business that requires clandestine access and means. That virtually marries most of it to clandestine HUMINT.

Paramilitary CA is a special case, and one for which a considerable experience base exists. Two major problems have always beset it: who performs it and who controls it?

The first question has an obvious answer. High quality and extremely competent personnel are needed to perform it. Whether the Department of Defense special operations forces supply such personnel and equipment or whether the clandestine HUMINT service builds its own capabilities has long been the disputed question. It does not really matter which agency does it so long as the quality of the capabilities is high. In practice, however, CIA has never given paramilitary capabilities the priority they need for them to be high quality. The increasingly technical aspects of CA make this deficiency greater today than in the past. Paramilitary operations, of course, are primarily "military," not clandestine HUMINT. Thus the professional expertise for paramilitary operations in the CIA has not tended to be great, especially in overall conception and command. Military affairs have grown far more complex, and keeping up with them has been difficult for the CIA.

The second question concerns control. Clearly in peacetime, the DCI, with his authority over clandestine HUMINT, is the proper person to direct and control such operations. In wartime, however, the need to integrate paramilitary operations within theater military operations puts the unified commander in the best position to control paramilitary CA. He also needs to have a say in non-military CA during wartime. The

official government policy has generally followed the principles suggested here, but the DCI and CIA have not always been willing to follow that policy. This issue needs to be settled, once and for all.

To sum up, CA is not an intelligence operation. It is either a “policy” operation or a “military” operation. The IC, of course, has to support it. Within the IC, the distinction needs to be redefined, bringing the Secretary of Defense, the Joint Chiefs of Staff, the Secretary of State, and the White House into the primary control role. Policy and military operations are their primary responsibility. When they turn it over to the IC, ambiguities are inevitable, and responsibilities remain unclear.

Information Warfare (IW), a recent fad of considerable future importance, would seem to overlap in some ways with CA and deception operations. IW, therefore, is another organizational and policy problem yet to be sorted out. Sufficient practical experience from which to generalize has yet to be acquired, but the issue needs to be on the IC agenda. It clearly is an “operations” and “policy” function as opposed to an intelligence function, but it requires enormous and complex intelligence support.

The problem of security against hostile IW is wholly new to the CI community. The IC today simply does not have the technical skills for providing needed CI support against IW. Nor is the primary national-level CI agency, the FBI, ever likely to acquire them. Neither CIA’s CI nor the FBI under tasking control by the Defense Department is likely to work in a way that allows effective intelligence support to IW from either CI agency.

Deception. Deception operations are important, especially in wartime military operations, but not necessarily confined to them. They depend heavily on intelligence capabilities of all types, and that sometimes leads to treating them primarily as intelligence operations, especially clandestine HUMINT operations. Yet they can seldom be contained within the clandestine service because key officials outside of the IC may have parts to play. They can be viewed to some degree as CA, but are “deception operations” a form of “covert action”? The military services have not thought so. This an ambiguous area yet to be fully sorted out.

Security. Although security is clearly a command and management responsibility, it requires strong intelligence support, and strong CI of the type most CI organizations do not really understand. Again, the example of technical penetrations of the U.S. Embassy in Moscow showed the weakness of the security system. Neither technical CI capabilities in State nor in CIA were adequate to discover them, much less anticipate them. NSA finally did. The lack of clarification of technical CI support responsibilities led to endless and non-productive reactions to the discoveries.

Development and production of communications security (COMSEC) and computer security (INFOSEC) are the responsibility of NSA. This puts them within an IC agency. Both areas are confronted with huge challenges by changing technology in the civilian community and abroad. Difficult legal issues confront both. Interagency turf issues have been fueled by the questions of well-intentioned Congressional committee chairmen, e.g., then-Congressman Jack Brooks’ effort to put a large part of INFOSEC responsibility in the Commerce Department.

These four functions—covert action, information warfare, deception, and security—will be treated only cursorily, if at all, in this study. Spelling out their place in this paradigm, or doctrine, for intelligence operations is necessary, nonetheless, in order to show why they are largely excluded. They transcend the IC although the IC has important supporting responsibilities for them, and even execution responsibilities in some instances.

Resource Management

Resource management (RM), of course, concerns the acquisition and use of funding. It can be broken down into two separate but related functions. The first is programming and budgeting efforts through which budgets are developed for submission to the Congress. The second is budget execution, that is, obligating and spending the monies appropriated by the Congress in accordance with the laws authorizing the appropriations. At all times, the RM task of the IC consists of dealing with three budgets: 1) programming and budgeting submissions to the Congress for the following year; 2) defending the program budget (built in the previous year) before the Congress; and 3) executing the budget most recently approved by the Congress. All IC agencies are deeply involved in RM.

The DCI controls the first function, programming, budgeting, and presentation to the Congress of the budget for entire national-level IC. The national-level IC is funded by the National Foreign Intelligence Program (NFIP). Programming and budgeting for the Joint Military Intelligence Program (JMIP), or Defense-wide intelligence programs, are carried out by the Department of Defense, although the DCI now works with the Deputy Secretary of Defense to develop and issue joint programming guidance for JMIP. Tactical Intelligence and Related Activities (TIARA) fall to the military services for programming, but again the DCI works with DoD to develop and issue joint programming guidance. The DCI uses the CMS as his resource management mechanism for the NFIP. While the various parts of the IC, located in several different departments and agencies, formally submit their budgets directly to Congress, the DCI and his staff have the responsibility for integrating and approving those budgets. Intelligence agencies each present their part of the NFIP. After approval by the DCI, agreement by the department heads, and endorsement or alteration by the Office of Management and Budget at the White House level, the budget request goes to Congress for approval.

The second function, budget execution, is left to the departments and agencies. The DCI is not in charge of IC budget execution. In a very few cases, he may play a consulting and persuasive role, but each statutory IC agency, or its parent agency, actually spends the budget under the rules of its parent department.

This system of allowing the DCI to build a consolidated interagency program and budget proposal has grown up in an evolutionary manner, and it is a considerable achievement toward giving the DCI the authority to prevent duplications among departments in intelligence resource management. How effectively various DCIs have used this authority is an important issue for investigation, but in principle the DCI has the authority to direct cross-department rationalization of the programming of resources.

At times, when IC reform legislation has been considered by the Congress, thought has been given to providing the DCI authority over the entire budget execution function [1]. While this idea has appeal for strengthening the DCI's powers over the IC, it is bureaucratically impractical. It would create duplication of comptroller and auditing functions within several cabinet-level departments and the military departments within the Defense Department. The inevitable turf disputes and management complications would far outweigh any advantages the DCI might gain from holding the powers of IC budget execution. Furthermore, such an arrangement might even be ruled illegal if reviewed by a court. Moreover, the DCI's program management authorities in building the NFIP have by no means been fully exploited. The major task for

contemporary IC reform, therefore, is making more use of the DCI's program authority, not expanding that authority to include budget execution. All the RM principles discussed henceforth, therefore, concern the first function, programming, not the second, or budget execution function.

The vertical rationalization of programming of resources is another matter. By the term, "vertical," we have in mind "national" intelligence capabilities and their relationship to "tactical" intelligence capabilities—the higher departmental capabilities versus the lower echelons of the military services. Quite naturally and logically, The Office of the Secretary of Defense (OSD) dominates the programming of intelligence resources at the Defense-wide (JMIP) level, and the military services dominate the programming of resources at the "tactical" (TIARA) level. In the military services, drawing a resource line between (a) capabilities allocated to purely intelligence activities and (b) dual-use capabilities—both combat operations and combat intelligence—is not easy. A naval surface combat vessel can collect intelligence. A combat attack aircraft can do the same. In ground operations, rifle squads may be dispatched on "reconnaissance" missions. Entire companies, or even battalions, can be deployed primarily for intelligence collection missions. "Reconnaissance in force" is the term for such use of military units normally dedicated to combat operations. Target acquisition systems for artillery and air support operations are not normally thought of as "intelligence" systems, but they can collect intelligence. Managing the programs within the Defense Department's tactical intelligence budget, therefore, involves ambiguous situations where capabilities cannot be clearly defined as either "intelligence" or "operational." The DCI's program management authority has never extended vertically, downward, to take account of these so-called "TIARA" capabilities.

Integrating the NFIP with the JMIP or TIARA will not be an issue in this study. It will be touched on, and there is much room for improvement in it. Trying to sort out all its complexities would require a separate analysis. Very large budgets are spent on the JMIP and TIARA, and this has properly prompted calls in Congress for better integration of the three budgets. One point, however, is axiomatic: Until greater resource management rationality is achieved within the IC in the National Foreign Intelligence Program, progress in integrating TIARA and the JMIP with the NFIP has limited prospects. This study, therefore, contributes to dealing with the TIARA problem, but it will not address it directly. The same is true for the Defense Airborne Reconnaissance Office (DARO), a rather recent organizational attempt to tie together development of aerial reconnaissance systems under central management.

Linking inputs to outputs. The key issue for RM is understanding how inputs of money (and personnel) relate to actual outputs of organizational product, which, in the case of the IC, comprise intelligence that is used. Since the time of the McNamara revolution in the Pentagon, when PPBS (Planning, Programming, Budgeting System) was introduced, there has been a general recognition of the need to relate resources more effectively to missions, that is, the "input-output" relationship. Budgets approved by Congress are organized on the "line item" principle. Line items, however, tell one very little about the input-output relationship. PPBS has been imposed on top of the line-item DoD budget in an effort to group budget lines with the missions they support. In effect, a dual system is used, first, "programming" for "missions," and second, line item budgeting for Congressional approval, fiscal accounting, and budget execution. In Congressional authorizations and appropriations, the "line-item" budget is law. Thus it must remain a given. To make a more rational connection between military budgets and output capabilities, the PPBS

system has been added, looking at the budget line items broken out as they relate to missions—e.g., strategic force missions, conventional force missions, and so on.

The Defense Department treats intelligence as a “mission” and tries to program for it in three categories: a) its part of the NFIP; b) the JMIP; and c) TIARA. As the manager of the NFIP, the DCI has never made the same effort to impose PPBS principles on resource management in the IC. Accordingly, the DCI faces a programming process in building the consolidated IC budget that does not effectively relate inputs to outputs. While a degree of “PPBS talk” normally transpires at Intelligence Community Executive Committee (IC/EXCOM) [formerly National Foreign Intelligence Council (NFIC)] meetings on the budget, no management and programming system has been devised to support the talk about input-output relationships.

For the doctrine of RM postulated here, therefore, we shall assume that the principle of PPBS, relating inputs to outputs, should be the rule. That raises the question of how to do it in the IC.

The obvious way to begin is to look at the main “functions” specified for the intelligence cycle. Those functions are, to repeat: a) collection management, b) collection, c) analysis and production, and d) dissemination. Two of these, a) and d) are “command and control” functions. The final output function is c). What comes out from the d) function is the most important measure of the IC’s output, but with a qualification. The output disseminated cannot really be counted unless it is used by policy-makers and diplomats and by military commanders and their operational staffs. Answers to questions that no one is asking or in forms that cannot be used often emerge from the intelligence process, but they cannot rightly be counted as “outputs.”

The major question, therefore, for the DCI to answer in his resource management responsibility is whether or not the IC’s output is used and actually meets the needs for policy and operations. And the IC organizations in the best position to answer that question are the staff intelligence sections in all military units and in the civilian departments and agencies where intelligence is relevant to their operations.

It also follows that intelligence production, if it is to be usable, relevant, and sensitive to the needs of users, must be done close to, and in constant working contact with, the users and their staffs. The military paradigm here is instructive. The concept of a staff intelligence officer, a “G-2” or (in unified commands) a “J-2,” envisions that “collection management,” “analysis,” “production,” and “dissemination” are accomplished by the G-2, J-2, and equivalent staff sections in Air Force and Navy units. The same idea is behind the existence of an intelligence section in the State Department, INR (Intelligence and Research). Similarly, most civilian departments and agencies have staff intelligence sections.

The White House as a “user” of intelligence is a special case that deserves additional comment. NSC staff members are normally the people who integrate most of the available intelligence products with the policy-making process in the White House. NSC staffers use raw intelligence from all collection disciplines and also a few of the many available finished intelligence products. This reality is somewhat at odds with the popular image of “all-source finished intelligence” produced within the IC and going personally to the President who reads and integrates it with policy decisions. This erroneous image posits the National Intelligence Council (NIC), supported by the CIA’s Directorate of Intelligence (DI) as a kind of national-level

“J-2” chief intelligence office for the White House. Finished intelligence products of this sort periodically do reach the President, and occasionally he is influenced by them, but these are exceptional and usually marginal influences.

The daily deluge of raw and finished intelligence into the NSC staff is the major influence that the IC has on the President’s view of the outside world. And even this competes with the mass media, individuals inside and outside government whom the President consults, and foreign leaders and officials who give the President their views and other information about foreign, economic, and military affairs. To the extent there is an intelligence staff section within the White House, it is the NSC Staff.

The above discussion leaves b), the “collection” function still to be addressed with regard to the input and output measurement questions. Collection is best considered by discipline: HUMINT, IMINT, and SIGINT. And CI collection is sufficiently distinct in many of its aspects to demand separate treatment for RM purposes.

From the resource management viewpoint, each of these distinct collection disciplines can be treated as autonomous input-output entities. The kinds of inputs for each include many common elements, but they also include many specialized elements unique to each discipline, making the input-output relationships in each discipline significantly different. Applying the PPBS principle, each of the three disciplines can be seen as program-mission areas.

The managers of the HUMINT discipline are in the best position to make judgments about what levels and mixes of resource inputs produce more or less HUMINT output. The same is true for IMINT and SIGINT. The measurement of their output, however, cannot be their prerogative. The policy and military users alone are in the best position to do that. In other words, resource managers face a large community of customers, spread throughout the civilian and military departments at the national level and even more at the lower levels in the military system of unified commands.

Budgets for the IC, like military budgets, are broken down into three categories—1) operation and maintenance (O&M); 2) procurement; and 3) research, development, testing, and evaluation (RDT&E, hereinafter referred to as R&D). Congress insists on these categories, and the IC must operate with them.

The management of the three budgetary categories tends to fall to separate and sometimes autonomous subunits. Managing R&D requires different skills and organization than does managing O&M. Procurement also requires specialized organization, skills, and management. Intelligence outputs, however, depend on inputs to all three. Applying the PPBS principle, then, at various levels of organization, management must work across all three categories, relating inputs for all three budgets to the output results of “intelligence operations.” Inevitably, organizations that carry out only R&D and procurement develop their own subunit interests that conflict with the interests of intelligence operations organizations and their O&M budgets.

Here we run into a major organizational and management tension between R&D and procurement organizations and those that primarily undertake operations, spending O&M funds. The input-output relation, that links them, conflicts with the internal organizational dynamics of each. R&D organizations

may prefer to pursue certain technologies that O&M organizations do not favor. And procurement organizations will develop compelling rationales for procurement efficiencies that conflict with both R&D and O&M organizations' efficiencies. Over time, parochial bureaucratic self-interest in each type of organization will begin to hurt both overall and individual organizational efficiencies in making better use of limited aggregate budgets.

It should be noted that all IC organizations and their subunits cannot be neatly labeled as purely R&D, procurement, or O&M. All have some O&M budget, some have a procurement budget separate from O&M, and some have all three. Still, R&D and procurement tend to be heavily lumped in specialized organizations that are not "operational" in the sense of being a collection organization. A serious organizational pathology is the tendency of R&D and procurement organizations to insert themselves into some part of collection operations in a way that keeps managers in collection organizations from having adequate control of the collection operation. The most glaring example is the NRO. And likewise, purely collection organizations respond by trying to conduct their own R&D and procurement.

A major bureaucratic cause of these organizational pathologies is the process by which programs and budgets are developed and approved. A fixed total figure for the budget is given at the beginning of the process. Each organization competes for its share in a zero-sum game. What any one gains is a loss for others. At times, the most effective allocation among the budget categories may be a large O&M budget at the expense of procurement and R&D. And at other times, vice-versa. And so on, through a range of mixes. The best mix, of course, depends on the kind and quantity of intelligence output needed to satisfy users. The game of the program budget building process naturally shoves that input-output viewpoint aside. Each organization's success, in its own eyes, tends to be the size of its budget. But those intelligence organizations most closely tied to intelligence users, also face pressures for direction of resources which are sometimes at odds with the zero-sum game of the programming process. Those with the least direct responsibility to actual users of finished intelligence are much freer to pursue their own budgetary goals.

Thus the staff intelligence producers and the suppliers of collected raw intelligence are closer to the final output side of the intelligence cycle and tend to feel the tensions between the two success criteria, effective output and size of their budget. The R&D and procurement organizations tend to be far more responsive to the budget size criterion.

There are no management panaceas for these tensions and dysfunctional behavior patterns. In general, however, single management across the three budget categories is preferable at levels where the cross-organizational input-output relationship is easier to assess and, therefore, to give priority among the budget categories. The greater the separation of organizational structures for R&D, procurement, and O&M, the more difficult and less effective will be the management of the input-output relationship.

As a general rule, managers at intermediate and lower levels will have better prospects of improving input-output relations if they have control of all three budgeting categories within a collection discipline. At the same time, managers at these levels will often refuse to take significant R&D risks and a longer view because they feel the daily pressures for delivering intelligence to analysis organizations and directly to users in some cases. Their view of the "long run" future, when R&D investment may pay off, is like Lord Keynes' comment, "In the long run we are all dead."

Subordination and Autonomy for Intelligence Agencies

Another doctrinal issue of fundamental importance for intelligence reform concerns the degrees and kinds of subordination and autonomy intelligence agencies should have. Is an intelligence activity so unique that it demands special organizational autonomy? Or is it likely to be more effective when its performers are organically subordinated to user organizations? Arguments have long been made for both as well as against both.

Organization theorists would probably conclude that wholly independent intelligence agencies have greater tendencies toward parochial self-interest at the expense of their primary goal—supplying timely and usable intelligence products. When they are directly subordinate to users, they are more likely to be responsive to the users. The users in that arrangement have greater control over their budgets, a lever that can be used to make them more responsive.

Another way to make this same point is to take other “general staff” functions from the military paradigm—e.g., personnel (J-1/G-1), operations (J-3/G-3), and logistics (J-4/G-4)—and try to imagine them as based outside the military command they support, formally required to respond to that command’s requirements but informally and bureaucratically able to neglect a full response without much fear of retribution or loss of resources. If the military services depended on an autonomous federal agency to run their manpower acquisition and promotion systems, it would soon become a national scandal. If special outside agencies were created to draft operations orders and war plans, how long would military commanders endure that arrangement? If they depended on non-Defense Department agencies for logistical support, how would that work?

All these examples would generate huge problems. At root they would all arise from the absence of control over resources by the user commands. Each autonomous supporting agency would have a separate budget and defend it in the Congress. Keeping those budgets up would inevitably become more important to each than satisfying the military commands they supported. If a particular unit or kind of support—let us call it “x”—could be provided in several different ways, and each way, based on different inputs and technologies, costs different amounts, the autonomous agencies would predictably prefer to use the most costly approach. It would require a bigger budget and more purchasing from private sector vendors, or more personnel, or both. The private sector lobbies would push Congress toward the expensive solutions, and the bureaucratic rank structure of the autonomous agencies would encourage them to seek the same solution. But if these agencies were subordinated to their users, they would face pressures to seek less costly solutions. The NRO, of course, is precisely such an agency, not dependent on funds from users of the systems it acquires, and therefore inclined to the most costly solutions, including solutions that users do not want at any price.

To make the point more forcefully, suppose that single family households were forced to sign up to a household maintenance organization for all their needs—electrical repair, plumbing, roofing repair, painting, lawn maintenance, et cetera. Rather than a private sector service-buyer and service seller relationship, suppose that this maintenance organization went to the Congress for its budget and the heads

of the households had to pay a federal tax to support federal funding of the maintenance organization. The maintenance organization would be pushing for higher budgets, and the heads of households—a diffuse and not easily organized potential lobby group—would be opposed to higher budgets. The intense and concentrated lobbying by the maintenance organization would probably defeat the heads of household lobby. The real-world example of this arrangement, of course, is Medicare. The Medicare budget began at a modest level but soon developed a dynamic beyond easy political or organizational control. This is precisely the phenomenon to be expected in the case of highly autonomous intelligence organizations.

The predictability of this kind of dysfunctional organizational behavior is so great that one has to be puzzled that autonomy for intelligence organizations has been allowed in a few cases. Yet there are reasons for it.

First, the oldest argument is based on the tendency of subordinated intelligence organizations being subjected to biases in analysis and reporting dictated by their users. The Pearl Harbor experience, it will be remembered, was cited after World War II as an example in support of granting the CIA a wholly autonomous status. There is something to this argument. Users, and not just military users, do not like to receive intelligence analysis that messes up their preconceptions and favorite policies and plans. In wartime operations, however, they tend to be more attentive to bad news because they may face defeat in combat if they reject candid and valid intelligence. Still, examples can be cited where commanders and political leaders ignored accurate but unhappy intelligence findings. Intelligence organizational autonomy, therefore, is not always a sure remedy to this problem. Several examples in assessments of Soviet military capabilities, defense spending, and diplomatic aims are evidence for that conclusion. Autonomous intelligence organizations themselves take on biases in their analysis, creating another source of distortion.

No organizational solution to these biases—user biases or intelligence analyst biases—offers a panacea. They are finally corrected by one or both of two factors. First, an adversary's actual behavior will eventually expose an intelligence bias. Second, individual analysts and intelligence officials sometimes stand up against institutional biases to make an objective case based entirely on a revealing analytical interpretation. Only the first, the adversary's behavior, is always a reliable corrective, although sometimes an extremely costly one. The second, honest and insightful intelligence officials, are problematic. More will arise, if the intelligence culture encourages them, fewer if it discourages them. One of the more perverse kinds of behavior among intelligence officers is assertion of autonomy to defend their integrity coupled with poor analysis, lack of insight, and simple misunderstanding of the evidence. Autonomous intelligence agencies will always be victims of such people, despite their honesty and good intentions.

Another corrective often proposed to solve this problem is so-called "competitive analysis," or the example of the A Team versus the B Team case in 1976 when an outside team was allowed to assess Soviet military capabilities independently. This corrective has yet to demonstrate its efficacy, and it has long been institutionalized in the competitive analysis among agencies like CIA, DIA, INR, and the military service intelligence chiefs. The result was seldom better analysis and frequently intense parochialism in spite of clear evidence being available to refute the positions of all the parties to the quarrels. Competitive analysis, as a rule, creates more heat than light.

The proponents of competitive analysis sometimes cite the academic community where scholarship supposedly is allowed to air all competing ideas in an honest marketplace for the truth. In the pure and applied sciences, this is most often the case because the standards of truth are not so ambiguous, but even the world of university science has its cases of fraud. In the social sciences, where the standards of proof are almost always ambiguous, misconceptions gain currency and strong institutional support allows them to persist, unsuccessfully contested, for long periods.

None of the arguments of this sort—from the Pearl Harbor example to the university world of competitive scholarship—add up to a compelling case for autonomous intelligence organizations. This is mainly true because the arguments are based on a misunderstanding of the world of scholarship. Truth in scholarship depends in the first instance on a combination of individual integrity and genuine insight. It thrives not because universities offer truly effective market places for ideas. Rather it thrives because senior scholars occasionally have the integrity and self-confidence to encourage younger scholars to do innovative and creative work. They sponsor them rather than compete with them. In intelligence analysis units, one occasionally sees a similar kind of behavior. A senior intelligence officer will recognize a subordinate's insight as valid although it conflicts with the senior's favorite answer to a question. Accordingly, the senior official sponsors and adopts a new conventional wisdom.

The intelligence user also frequently plays a critical catalyzing role in encouraging this kind of behavior among his intelligence staff officers. He takes a strong interest in the analysis but a dispassionate one, letting his intelligence analysts know that he is more interested in the unvarnished truth than in a preferred truth. He is tolerant of mistaken analysis if it is not defended in a parochial fashion, perhaps even rewarding the mistaken analysts who readily surrender their hypotheses when the evidence tends to undercut them.

No organizational technique or structure will ensure this desirable kind of behavior among either intelligence officials or users. We have to live with this condition although certain kinds of organizational management approaches can mitigate it.

Are there no good arguments for autonomy of intelligence organizations? Yes, there are. Complex technology and specialization of skills are the bases for the best arguments. A very old example is cryptanalysis, breaking communications codes. The number of people who can master cryptanalysis at a level that is productive for SIGINT has always been small. H. O. Yardley's infamous "American Black Chamber," set up during World War I by Colonel Van Deman, the Department of the Army G-2, was the first modern and highly effective cryptanalytic endeavor. It was a highly centralized and autonomous organization, but its products were distributed not just to military users. Diplomats became voracious consumers as well, and the 1921 Washington Naval Conference's arms control treaty was critically shaped by Yardley's products. Later, in World War II, SIGINT based on cryptanalysis was highly centralized and autonomous. The results have become fairly well known as remarkably effective. That effort, jointly shared with the British at Bletchley Park, England, although somewhat autonomous, was under the command of the Supreme Allied Commander, General Eisenhower. Thus he and his staff were in a position to limit its autonomy where it concerned dissemination and use. Lower-level commanders received its products, and enjoyed the advantages it provided. They probably realized that each of them could not have had an

organic cryptanalytic unit capable of the same quality of output; technically it would have been impossible. Centralization and greater autonomy for that cryptanalytic organization, therefore, made sense.

Still, SIGINT was also produced at the tactical level by units organic to lower command levels. Commanders could direct these units' efforts wholly toward their own intelligence requirements.

Another relevant example of organizational differentiation and autonomy at the *apparent* expense of the supported command is found in artillery. Any military commander tends to prefer organic capabilities rather than outside support because he knows organic units will be more responsive. Technology changes, however, frequently favor specialization and a non-organic relationship with commands that are supported. As the range of artillery increased, and as methods of fire direction and control advanced technologically, centralization of command over artillery at higher levels were essential for exploiting those technological changes. Brigades and regiments gave up "command" of artillery, and doctrine for "direct support" and "general support" were designed to let the higher-level commanders—at division and corps—allocate artillery support more effectively for their operations. Lower-level commanders did not like the change, but practice proved the advantage of yielding organic control.

The changing methods of tactical air support and strategic aviation reflect an analogous organizational response to new technology. Extensive doctrinal procedures for providing close air support to ground operations have been developed. Problems have persisted, however, over Air Force funding levels for close air support capabilities. Still, doctrine for providing close air support has been developed and used to reasonably good effect without ground force commands possessing organic tactical air units. Logistics, medical, engineer, and many other special capabilities have experienced similar changes.

These non-intelligence examples hold great relevance for intelligence organization. A degree of autonomy and specialization in organization offers tremendous advantages if it is accompanied by changes in doctrine for operations to ensure support for the command levels that surrender organic control. Intelligence has experienced vast technological changes and a great deal of organizational specialization and autonomy. It has not, however, kept up in altering doctrine for ensuring effective support. As a result, some of the organizational specialization and autonomy has been counterproductive. Early, the distinction between "command" and "OPCON" was made with regard to controlling intelligence collection assets. Examples of its successful application in SIGINT were noted. In the provision of intelligence support by non-organic, specialized collection organizations to users, a similar principle could be borrowed from the artillery examples of "general support" and "direct support." National-level collection and production of SIGINT has been provided on a *de facto* principle of "general and direct support," based on priorities determined by the Chairman of the Joint Chiefs of Staff. He and the Joint Staff decide which unified commander is to receive priority in a crisis or for some other special and temporary operation, and then NSA concentrates assets on that basis, taking support away from other unified commands during the crisis. This is precisely how division and corps commanders mass their artillery for greatest effect.

It must be emphasized that in all of these examples of technical specialization leading to organizational autonomy, the autonomy must be limited for effective intelligence. Somewhere up the chain of command, the most effective intelligence operations are subordinated to user commanders or policy-makers. That principle has come close to serious violation, however, with the creation of an intelligence agency at the national

level, subordinated only to the White House, i.e., the CIA. The White House is unlike any cabinet or other independent department. It has never been considered a “managing” agency, rather a policy-making agency that implements policy and operations through cabinet departments and agencies. There may be compelling reasons to maintain CIA as one of those implementing agencies, largely independent of all the agencies it is supposed to support, but the problems with the CIA over the last two decades demand that those reasons be re-evaluated to see if they really are so compelling. Why DCIs have not always forced CIA HUMINT to be fully responsive to military requirements, especially during crises, is a question needing investigation. It may be that they simply do not have the administrative capacity to compel it. It may be that his double-hatting as CIA Director encourages him to take a highly parochial CIA bureaucratic view. The same need not be true for the DCI and his CMS or some sort of analytic body such as the NIC. If anything, the DCI’s role as the national program manager and the national intelligence requirements and tasking manager has not been fully exploited. If the DCI’s NIC and its forerunners can be criticized for poor national intelligence estimates and interagency intelligence production coordination, that does not prove unambiguously that the function is not needed, only that it has not always been done well. Sponsoring competition among the analysts of the CIA/DI, DIA, the State Department’s Bureau of Intelligence and Research, and the military services has hardly been vindicated, although having at least a small analytic capability to take a national view has merits not so easily dismissed.

The organizational reform answers to the accumulating problems will not be found in generalities like “competitive analysis” or references to the Pearl Harbor experience. Rather they can only be discovered by investigations based on in-depth knowledge of technology and operational and policy-making processes. And they require more than a little trial and error through actual practice. At the same time, both investigatory analysis and practice need not be entirely unguided by some *a priori* concepts.

The doctrinal principles sketched out here are meant to provide such concepts. They are not immutable, and they are not *a priori* in the sense of having dropped out of the sky. Rather they are inductively arrived at, based on looking at what seem to be enduring effective paradigms of organization and functions in intelligence activities over a long period of time—most of the 20th century. Just as “fire and maneuver” have long remained enduring principles in military operations even as military technologies have changed radically, the intelligence cycle and collection disciplines have remained continuously valid.

A final point about subordination and control concerns the military character of intelligence operations. In this effort to set forth a general doctrine, or set of organizational principles, the military examples have been dominant. That is not accidental. Intelligence has always been closely, even primarily related, to military operations. Diplomacy, of course, also has long been associated with intelligence. At root, however, intelligence operations have a closer affinity to the military ethos than any other. First, they are competitive and generally operate outside traditional legal systems, both domestic and international. Attempts at regulating war through international norms and laws can, at best, yield limited results. Intelligence activities, however, have not been the subject of these kinds of multilateral efforts toward regulation. Even so, they are truly war-like. Spies risk and lose their lives, just as soldiers do. The same is not so true for diplomats, although they take exceptional risks at times.

Civilian control of the military is a fundamental axiom of the American political system. Given the military-like character of intelligence operations, to what extent is that axiom valid for intelligence organizations outside the military services and the Department of Defense? To the greatest degree. The issue, however, is not really “civilian” control in the sense of uniformed military versus civilian control. It is really a matter of political accountability. Civilian bureaucrats and lower-level political appointees in the Defense Department are the true source of civilian control over the U.S. military. The real control is “political,” responsibility before the electorate. The Congress’ control over the budget is the core element of that support, and the power of the voters over the President and the Congress stands behind the powers of the purse. Presidentially appointed officials in the Defense Department exercise the President’s political control over the military just as the Congress controls it through the budget. The President does not know personally very many of the scores of his appointees in the Defense Department, and his capacity to know whether they actually are fostering his policies is even more limited, probably reaching down no farther than a handful of people below the Secretary of Defense. The others can hardly be called the foundation of civilian control over the military, and thousands of civil servants in the upper reaches of the Pentagon are not even bound by the ethos of a military officer’s responsibility to the constitution and political authority, an ethos cultivated from the very beginning of an officer’s training.

These observations are made to anticipate the argument often made that the CIA, as a “civilian” agency, effects “civilian control” over intelligence operations that would not exist if they were carried out by military personnel. This is clearly a false argument. There is indeed a problem of political control over intelligence operations, but it has nothing to do with clothing, military uniforms versus blue or gray flannel suits. In fact, the principles of military officer training—duty, honor, country, and dedication to the principles of political authority based on the constitution—would at least be a psychological control factor for an independent intelligence agency like the CIA. Its civilian personnel, however, are not subjected to sufficient amounts of this kind of socialization and character training before being posted as intelligence operators and analysts; the re-training they receive as their careers progress appears to be even more sporadic.

Political control over the CIA, therefore, is a serious issue, a growing problem, but not because military officers are in charge. The DCI and sometimes his deputy are the only political appointees acting for the President in controlling it. This issue, therefore, deserves scrutiny, but not in the sense that it is normally raised.

Another variant of this civilian-military issue concerns the presumed propensity of military intelligence officers to short-change non-military intelligence needs. The grounds for this worry are difficult to find. The National Security Agency, according to DCI William Casey, supplied about 80% of all national intelligence needs in the mid 1980s. Well over twenty civil agencies depend heavily on its collection. Few if any of them complain about being short-changed. Yet NSA is commanded by a military officer, and more than two-thirds of the personnel working under NSA command or OPCON are military. CIA and the FBI are wholly civilian agencies but have much poorer records of satisfying civil agency users. And DIA, a military organization, has no record of turning down civil agencies’ requests for intelligence although not many ask. In fact, DIA has vigorously pursued the distribution of its products to the White House and to any other

non-military user who will accept them. All in all, the fear that military intelligence agencies will not respond to the DCI's tasking and distribution of products to non-military agencies seems groundless.

Intelligence Management Training

Introduction

Even if a common doctrine for the IC were promulgated as official policy, the IC's behavior would probably change very little without comprehensive and recurrent management training. That is because few senior intelligence officers—military and civilian—today know enough about the entire IC structure and operations to apply a common doctrine. Senior management training, therefore, is desperately needed. This applies not just to resource management, where it is a major problem. It also applies to collection management. The intelligence officer on a naval combatant, if he knows how, can request and probably receive vast amounts of intelligence from non-naval intelligence collectors. The G-2 of an Army corps could do the same. Yet nowhere in the intelligence schooling system are officers headed for these assignments taught, or allowed to know, how they can request national and other outside collection support. The same is probably true of the collection management and analysis elements in civilian cabinet departments.

All components of the IC have training programs and education systems. Intelligence schools are especially numerous in the military services, and the DIA runs the Joint Military Intelligence College and the Joint Military Intelligence Training Center. The number of courses in photo interpretation, signals intelligence, clandestine trade craft, and special kinds of analysis is quite large. DoD's Defense Language Institute contributes to the IC through its many language training programs, and there are several other foreign language schools inside the IC. In short, the IC has a large, fragmented, diverse, and specialized system of education and training.

Undoubtedly much of this school structure could be improved, made more relevant, raised in quality, and made more comprehensive. That is a perpetual challenge faced by the intelligence schooling system, rather than an issue for systemic reform. The schooling system's performance is mixed, ranging from outstanding to fairly poor. In the technical collection disciplines it is always struggling to keep up with changing technology. In HUMINT and especially CI it is very uneven. In collection management, training is very poor except in some narrow technical spheres within the technical disciplines. Training in analysis and production is also mixed in quality. Among its greatest failings has been inadequate attention to teaching analysts how to gain access to all sources of intelligence. The university research analogy is knowing library and archive research and retrieval skills, and they are not always well taught. Most good analysts learn them on their own.

Major Deficiencies

The IC school system lacks three elements. First, nowhere is a common doctrinal understanding of intelligence functions and processes documented and taught to all IC management and executive

leadership personnel. Second, the teaching of IC-wide resource management has been generally neglected. Third, nowhere is senior executive leadership and staff training accomplished effectively for the IC. Let us consider each of these deficiencies.

An IC Doctrine. Earlier this section of this study elaborated a number of doctrinal concepts that provide a common language for understanding and organizing intelligence operations. Today, if a dozen or so senior officials from all IC components were pulled together and quizzed on these principles, they would not give compatible answers, and most would give non-sense answers. For example, “collection management” has many different meanings in practice, and senior officials from different backgrounds bring quite different understandings to this term. The same is true for most of the intelligence functions and for more specific language within collection disciplines. The result is a serious problem of miscommunication within the IC. Intelligence officers rise to very high posts with extremely parochial and limited comprehension of intelligence functions and processes. Yet they most often assume they “really know” the IC and intelligence as a profession. In fact almost none have a *comprehensive* view of the IC and its operations.

This state of affairs in senior management can be explained in part by the requirements for security compartmentation and limited, need-to-know, access to many IC programs. An official who grows up in the HUMINT discipline will inevitably have a limited comprehension of SIGINT and IMINT, and vice versa. Those with experience in tactical military intelligence understand aspects of intelligence operations that remain a mystery to more than 90% of senior management personnel in the whole of the IC. Likewise, many tactical military intelligence specialists know very little about national collection systems or providing intelligence support to civilian departments.

Even within the military, there is no standard doctrinal approach for joint intelligence staffs (J-2s). Collection management is performed differently in each. Staff sub-functions also differ between the joint intelligence staffs of the Unified Commands. By and large, each is an ad hoc arrangement. Little wonder that most of these staffs have difficulty drawing on all intelligence collection capabilities available.

The lack of common doctrinal understanding in CIA/DI has kept it in counterproductive struggles with virtually all components of the IC. At times, the DI has tried to take over virtually all IC collection management while the old IC Staff had that function officially. DIA has had similar turf fights with NSA and the J2s. When CENTCOM deployed to Saudi Arabia for the Gulf War in the fall of 1990, the J2's handling of collection management and analysis was rapidly changed on an improvised and ad hoc basis. CI, clandestine HUMINT, and IMINT have never easily adjusted to support military operations, precisely because what such support entails is not specifically spelled out and taught as standard procedure.

While this parochialism and limited knowledge may be explainable, it is wholly unacceptable among the senior ranks of IC leadership. Until it is overcome, this deficiency will continue to obstruct meaningful dialogue and cooperation within the top circles of the IC. A common doctrinal language has to be mastered by all senior IC officials, and it has to be updated continually in light of new technology and new operational concepts based on practical experience.

IC resource management. No less important than a common doctrinal language for the IC is a common understanding of IC resource management. The “Concepts and Principles” section raised a number of key

issues for resource management. They need to be greatly expanded and made the focus for training and education of both lower and higher resource management officials. Here again, the absence of a common language and set of understandings is a serious deficiency which IC education reform must address. This means more than technical training in “program management.” It also should include critical analysis of the levels of efficiencies in the present resource management techniques and methods.

Leadership and staff work. Just as most large organizations require senior management and leadership training, the IC desperately needs this for its civilian personnel. The senior military personnel in the IC have somewhat more leadership training in early- and mid-career schooling, but this training is not particularized to the IC.

More serious than lack of leadership training in the IC is lack of training in high-level staff work. In fact, even most military officers in the IC do not really comprehend what “complete staff work” is. Nor do they always understand the difference between “staff” functions and “line” functions. And they do not understand “staff parallelism” and “span of control” issues.

By comparison with the military personnel, however, the IC's civilian personnel are far less schooled in all of these matters. Most have been promoted to senior positions because of their acute bureaucratic skills, not their management and staff work skills. Simple organizational processes and principles, common to virtually all organizations, are very unevenly understood among the senior executive service civilians in the IC and not all that uniformly by senior military officers. Many civilians are sent to the military services' war colleges, but these schools are totally inadequate for the senior leadership needs of the IC.

Recommendations

- The DCI should create an IC senior management education system.
- This system should have as its core curriculum three areas: a) IC doctrine; b) resource management; and c) leadership and staff work.
- A simplified version of this curriculum should be required for entry-level and mid-career schooling of intelligence officers, as well as for senior-level officers.
- This schooling system should involve senior line and staff personnel as instructors.

Getting a competent faculty for intelligence schools is not easy. The best solution to this problem is to force the incumbents in most senior positions in the IC to devote significant time to teaching courses in the IC school system.

This management and leadership schooling is not a substitute for any of the present IC education or training. Rather, it must be added to current education, and it must be small and select at the top levels.

Conclusion

The many concepts, principles, and arguments presented here cannot be applied in a mechanistic fashion that will easily turn up all of the structural and procedural problems in the IC and provide solutions to them. They can, however, provide a common language for seeking them out and for distinguishing between remediable problems and unresolvable tensions and frictions. And they should, if pragmatically applied, lead to a set of recommended reforms that are mutually consistent and reinforcing, rather than largely ad hoc, incomplete, and perhaps even contradictory.

Note

1. *IC21* (p. 76) calls for giving the DCI limited authority to reprogram funds within the NFIP. The Intelligence Renewal and Reform Act of 1996 (Public Law 104-293—Oct. 11, 1996), requires the reporting to the DCI and the Secretary of Defense of budget execution data for all intelligence activities (Sec. 807).

Section III

The DCI Management Structure for the Intelligence Community

The inchoate outlines already exist for a management structure through which the DCI can direct and manage the Intelligence Community. They came about slowly, some of the parts appearing early, others emerging later. Particularly from the late 1960s through the early 1970s, the issues of managing requirements and collection priorities, of resource and program management, and IC-wide policies received attention. Over this period, the U.S. Intelligence Board—the predecessor to the National Foreign Intelligence Board—which approved “national” intelligence analytical products, and the Intelligence Community Staff—the predecessor of today’s Community Management Staff—began to take shape. The CMS deals not with intelligence analysis but with the plethora of organizational, budgetary, and policy issues pertaining to the entire IC. In the 1980s, the National Foreign Intelligence Council—now the Intelligence Community Executive Committee—was created to deal primarily with resource issues. NFIC membership overlapped with the NFIB but was much smaller and included officials not on the NFIB, namely the CIA deputy director for administration, the director of the ICS, and sometimes other ICS officials.

These organizational arrangements were designed to allow the DCI to perform some of the basic functions outlined in the “principles and concepts” section. The purpose of this section is, first of all, to identify and explicate the relevant functions from our general doctrinal approach. With that done, the current structural arrangements can be assessed and changes can be recommended that will strengthen the DCI’s management capabilities for directing the entire IC. The required structural changes, however, go far beyond the management organization directly supporting the DCI, and for that reason, some of them will be touched on sufficiently to show why they are critical for improving the DCI’s capabilities for managing the IC.

DCI Management Functions

In these developmental processes, three distinct roles for the DCI are discernible. They must be fully clarified and understood for any effective reform of the DCI’s role.

Collection Management, Intelligence Analysis and Production, and Dissemination

As the top intelligence official in the government, the DCI is responsible for producing intelligence analysis and judgments for the President and the cabinet-level officials, and at the same time, he has to deal with the conflicting intelligence analyses produced by various components of the IC. In other words, he has to “manage” intelligence production not just in the CIA and the National Intelligence Council (NIC), but

throughout the entire IC. “Management” is different from immediate “direction.” He clearly must “direct” the NIC’s analytic efforts and chair the NFIB in its role as the validating authority for national level intelligence estimates and other products.

Producing intelligence can only be done if information is “collected,” and thus the DCI has to provide “collection management” for the IC. First of all, he must deal with “non-time sensitive” collection management for the entire federal government. That requires a system for aggregating the requests—“intelligence requirements”—from all departments and agencies, prioritizing them, and assigning them as collection tasks to appropriate collection agencies. In the current system, collection management is performed by the CMS. Following our “principles and concepts” section, that function more appropriately belongs to the NIC.

Collection management and intelligence production, however, take place in scores of places, not just at the national level. Each cabinet department has its own special needs for intelligence products. In the Defense Department, the JCS, the unified and specified commands, and in the military services, the need for specialized intelligence products is highly varied. Below the level of the Secretary of Defense, virtually every military organization possesses its organic intelligence staff section to respond to its particular intelligence analysis needs.

The DCI, even with the NIC’s assistance, cannot possibly “direct” all of this collection and intelligence production. And he should not. The using policy officials and military commanders (who know best what intelligence they need) must “direct” it, assisted by their organic intelligence staffs. This, of course, reflects the “distributed processing” model of intelligence production mentioned in Section II. The DCI, however, can and should perform a general “management” role embracing most of this dispersed community of intelligence analysts. He can look for duplication, for analysis that is done without adequate access to collected intelligence, for lacunae in areas of analysis that are being neglected. And he can resolve disputes that affect national-level intelligence production. Finally, he can assure that the President, through the National Security Council Staff, is provided with whatever intelligence analysis it requests, as well as intelligence analysis he believes it needs but had not requested.

The DCI’s obvious staff support for IC collection management and intelligence production is the NIC. As the IC now operates, however, collection management is performed by the CMS, and the CIA/DI often assumes that it is the DCI’s primary intelligence production staff, and that in turn has prompted it to try to run collection management for the DCI. Not surprisingly, many dysfunctional turf quarrels have arisen as a result.

Resource Management and Policy for the IC

Three distinct management functions are housed in this responsibility. First, as the director of the IC, the DCI must evaluate the IC’s outputs. That requires a system for evaluating the fulfillment of collection management tasking, i.e., collection organizations’ responsiveness to “national intelligence requirements.” Second, he must manage resources, that is, supervise IC programming/budgeting and decide the allocation of funds and personnel. Third, he must make policies applicable to the entire IC.

The obvious vehicle for assisting the DCI in executing these responsibilities is the CMS. The CMS cannot support the DCI adequately if it is merely a “parliament” for the IC components, as it traditionally was in its earlier incarnation as the IC Staff. The CMS must be truly a staff, not a directive body. It must work out alternatives to deal with issues and tasks and present them to the DCI for decision. In other words, it must have a process that begins with problem identification, analysis of the problems, development of solutions, and presentation for the DCI’s decision. The decisions, then, are the DCI’s, and they take on the power of his directive authority.

The DCI’s responsibilities to “evaluate outputs,” “manage inputs” and “make policy” must be understood in the interdepartmental and organizational context of the IC. They should not be interpreted as giving the DCI authority to override, or interfere with, management and command within the Defense Department, the military services, and in other agencies with complex and deeply embedded intelligence structures. The very nature of the IC makes tensions unavoidable between the DCI, with his responsibilities for management and particularly for direction, on one hand, and the various departments’ managers and commanders on the other. Such tensions, however, can be kept limited if the DCI is not too literal about “direction” below the upper levels of the IC. In some cases, of course, his policies, e.g., security classifications and handling of intelligence products, must be accepted as unambiguous directives. But in other, less clear-cut issues, if the DCI brings the heads of the IC components along with him, they will help mitigate bureaucratic conflicts as well as make the DCI’s policies and management aims penetrate more deeply inside all independent departments and agencies of the IC. In fact, this “style of leadership” issue, achieving “community” within the IC, is sufficiently important to merit specification as a major and distinct aspect of the DCI’s office.

IC Coherence and “Community”

If there is to be a genuine sense of “community” within the IC, the DCI has to assert, foster, and exploit it. The NFIB has generally performed this role in matters concerning “national intelligence,” e.g., NIEs and other such products. On the management side, during the 1980s the National Foreign Intelligence Council, composed of the heads of the IC components, the director of the ICS, and a few others, served as a consultative body for the DCI before he made resource decisions. The NFIC (now superseded by the IC/EXCOM) never worked very well for a number of reasons, mostly concerning IC structure and NFIC membership. Such a council of the senior leaders of the IC, however, is essential. It can provide the DCI with advice on the wisdom and likely consequences of his decisions before he makes them. It can create a sense of IC institutional coherence, providing participation for heads of IC components from various departments and frequent, direct interaction with the DCI. This last point is extremely important because the interdepartmental nature of the IC makes the DCI’s executive role difficult. Some sort of cohesive council headed by the DCI can provide a vehicle that helps the DCI impart clearly the rationale and aims of his decisions throughout the entire IC. Not only will IC component heads be better able to implement these decisions; they can also better explain and defend them within their own departments.

Equally important, if an IC/EXCOM-like body is to work effectively, the CMS must be its staff organ, preparing its agenda, providing the staff analysis to support its deliberations.

Recommended Changes for the Position, Role, and Authority of the DCI

1. Make no statutory changes in the DCI's authority.

Formally the DCI's statutory authority is adequate. Perhaps some things, which are within his authority by virtue of precedent and practice but not necessarily in law or Executive Order, might be codified in one or the other form, but there is no pressing need for it. Two additional authorities have occasionally been strongly recommended. It is necessary, therefore, to explain why they are not advisable.

First, greater personnel control in non-CIA intelligence organizations has been proposed to include the DCI's right to select the directors of the DIA and NSA. The DCI does need to take an active role in IC-wide personnel policy-making. For example, personnel security clearances are granted on the basis of widely divergent criteria from agency to agency. Greater commonalty makes sense, and the DCI should try to achieve that. Education and training policies for the IC need DCI policy attention. These things, of course, can be done under the DCI's current authorities.

Appointing senior military officers to lead DIA, NSA, and now NIMA, however, is not within the DCI's prerogative, and it should not be. These defense agencies are within the military command system. Their directors are chosen from among flag officers by the Joint Chiefs. Very seldom does an incumbent DCI personally know the whole set of officers from which one must be chosen. The Joint Chiefs do. The director of NSA in particular is in a position precisely analogous to all the commanders of unified commands. No one would dare propose that some outside appointed official be allowed to interject himself into the military chain of command to select officers to become CINCs of a couple of unified commands. If the DCI had that authority, it would ensure permanent and deep resentment by the Joint Chiefs and unified commanders, making the DCI's management of the IC extremely difficult.

Most DCIs, when they have truly wanted to influence the selection of directors of NSA and DIA, have informally expressed their views to the Secretary of Defense and the Joint Chiefs. And they have normally succeeded in affecting these appointments with this approach. Neither the Secretary of Defense nor the Joint Chiefs are inclined to appoint an officer who is unacceptable to the DCI. When the DCI's first choice has been refused (and it has on occasion), he has usually been able to exercise an informal veto of candidates he strongly opposes. Given the "interagency" character of the IC, this informal exercise of influence over senior IC personnel appointments is much preferable to formal authority [1].

Second, giving budget execution authority over the National Foreign Intelligence Program to the DCI (in addition to program management authority) has been proposed at times by the Congressional oversight committees. From the oversight committees' viewpoint, this is understandable. It would simplify and strengthen the committees' watch over the execution of the intelligence budgets.

At the same time, however, it would complicate their relations with the armed services committees which are not inclined to share this oversight role. Far more complicated would be DCI management of budget execution inside each of the military services and inside the DoD for NSA, NIMA, DIA, etc. Budget

execution, by its administrative as well as management nature, must be done through a direct organizational hierarchy of responsibility and accountability. Having two overlapping budget execution authorities trying to manage jointly the spending of the monies would not only inspire endless bureaucratic turf quarrels, it would make responsibility ambiguous and accountability difficult. Thus giving budget execution authority to the DCI for every account in the IC budget would be a cure far worse than the disease.

"Program management," i.e., the building of a unified intelligence program to be presented to the Congress for authorization and appropriation, is another matter, and the DCI performs this task for the entire National Foreign Intelligence Program. This authority of the DCI is a powerful tool for deciding allocations throughout the IC. Once the NFIP is passed into law by the Congress, of course, agency discretion in budget execution is fairly limited. Thus the agencies of the IC are not at liberty to ignore the DCI's resource allocation preferences at will. If the DCI wants to exercise management approval of agencies' re-programming requests before submitting them to the congressional committees for legal approval, he can do that, using the CMS.

The major program management problem the DCI might face would be a decision by the Secretary of Defense to re-program funds within the DoD's portion of the NFIP. Here the Secretary's formal fiscal authority is stronger than the DCI's program management authority, allowing the Secretary to ignore the DCI's preferences if he chooses. In such cases there is no tidy administrative solution to what are essentially disputes between the DCI and the Secretary. If the DCI feels very strong about such a dispute, however, he has a route of appeal. He can ask OMB to take it to the President for resolution. This is the DCI's real source of bureaucratic power. Because the NFIP is, in reality, the President's budget, handled by OMB, the President can make the DCI as strong or as weak as he likes in managing the NFIP. It is difficult to see how new or different legal authorities for the DCI could improve the present situation.

The key changes in the DCI's status which are most needed are in his style and the clarity of his position as the DCI as distinct from the Director of CIA. If the CIA is to be retained, the DCI should reverse his traditional relationship to it, which is to be closely identified with CIA and loosely identified with the IC. This almost inexorably requires that the DCI not collocate his offices and personal staff, the CMS, the NIC, and any other special support structures with the CIA. At least, the DCI must make the separation conspicuous to the IC for symbolic purposes.

The temptation to increase the formal authorities of the DCI by statute is understandable although ill-advised. The Congressional intelligence oversight committees naturally tend to want the DCI to answer to them on the same basis as any federal agency head, cabinet level or lower. In reality, however, this is not possible because the IC is interdepartmental, and it cannot be otherwise. Intelligence, as our "doctrinal" section makes clear, is not an independent function that can be wholly autonomous from the organizations it supports. The IC and the DCI's control of it simply have to be viewed as a special case, cutting across organizational lines in an untidy fashion in many cases.

The changes that do make sense in light the DCI's two major areas of responsibility—1) collection management and intelligence production, and 2) resource management and IC policy—can all be made within his present legal authorities.

2. Strengthen the role of the National Intelligence Council as the DCI's instrument, for:

- overall collection management in the IC,
- providing analysis at the national level that is not produced by any other analysis agency or section,
- overseeing analysis and production in all IC components,
- overseeing and ensuring an IC-wide system of all-source data files and materials that are kept available to all intelligence analysis units.

Collection management would be a new function for the NIC. It belongs there, however, according to our "principles and concepts" doctrine. It is a staff function that initiates and directs the entire intelligence production cycle. Currently this responsibility resides with the CMS, and arguments can be made to retain it there. But because aggregating and prioritizing requirements are so closely related to what intelligence analysts need and what they should be doing, NIC personnel are likely to be better informed for carrying out this function effectively than CMS personnel, who are more distant from intelligence production activities. Figure 2 illustrates the reformed NIC's collection management role for the non-time-sensitive raw intelligence needed for intelligence production in the civilian departments.

The NIC, of course, cannot undertake most "time-sensitive" collection management, especially for military operations, and sometimes for political crises. NSA has a highly effective system for time-sensitive collection management challenges, and to a lesser degree, such a system exists in DIA to support the JCS. Largely these systems deal with SIGINT collection. IMINT and HUMINT have always been behind in responding to crisis demands for rapid shifts in direction of collection capabilities. Proposals for how this situation can be remedied will be addressed in the sections on IMINT and HUMINT. Here it should suffice to emphasize that the problem cannot be solved at the NIC level. The NIC should help the DCI ensure that time-sensitive collection management can be handled by each of the intelligence collection disciplines, but the communications, knowledge of collection sources, and the technical nature of actual directives for shifts in collection are complex and different for each discipline. That means that each discipline must solve them separately but within an IC-wide concept of collection management operations. Staff supervision in the design and creation of the collection management system does lie within the responsibility of the NIC.

In intelligence production, the DCI cannot be the only voice on intelligence judgments although he can be the final authority in disputes over national-level judgments. Every department has its own policy or operational issues which, if supplied adequate intelligence analysis, are beyond what the DCI can know about and for what he can be directly responsible. For example, neither the DCI nor the CIA/DI can know about or provide the comprehensive technical intelligence needed to support a Navy weapons program, or an Air Force aircraft R&D program, or an Army tank program. Even political intelligence needed to support decision-making by the National Security Council is seldom the monopoly of the DCI. The President's National Security Advisor and his staff are frequently better placed and informed for making key intelligence judgments. At times in the 1980s, the Secretary of State was far better informed about Soviet

leadership views than the DCI or any part of the IC. The Secretary simply spent so much time with Soviet officials—and his immediate staff aides interacted with Soviet Politburo members' staff aides—that

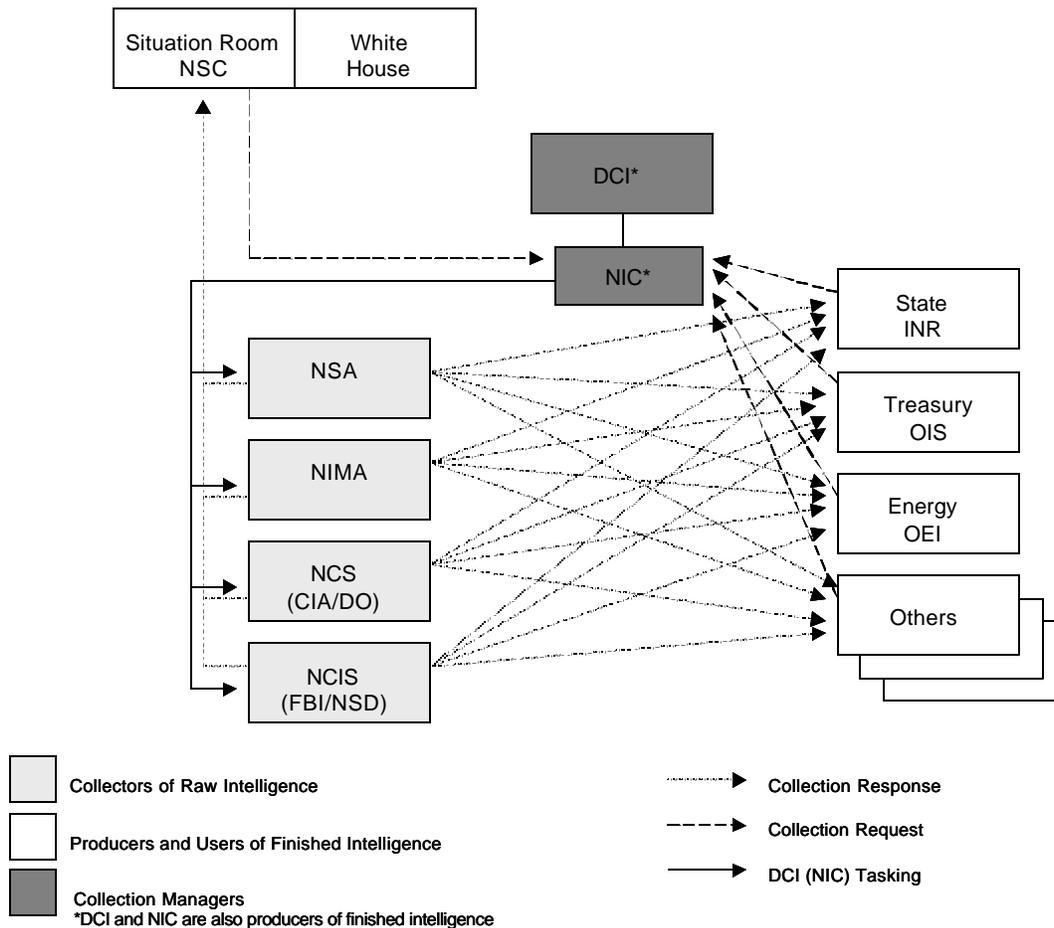


Figure 2. Reformed Collection Management and Intelligence Production for Civilian Departments

he had better insight into the top leadership circles. The Secretary of Defense at times is vastly better informed on foreign military matters by his own intelligence analysts than is the DCI. This is normal and to be expected, rather than a deficiency. In fact, an effective DCI contributes to this reality by ensuring an adequate resource allocation and an effective division of labor among intelligence production capabilities.

The NIC and its staff members, however, can range through the IC, staying abreast of the state of analysis and production, its strengths and weaknesses. Specifically they should perform the following functions:

- Identify gaps that are ignored because they seem to fall between agencies. Discover duplication. Identify analysis units that are not receiving relevant raw intelligence collected by HUMINT, SIGINT, or IMINT means. Assess the quality of analysis in various IC production units. The NIC cannot do all of these things down to the lowest levels, especially in the military services and unified commands, but at the higher reaches of these organizations it can stay aware of what is being done.

- Advise the DCI, based on the findings from these exploratory activities, on formal allocation of intelligence production responsibilities among all IC production organizations. Also recommend intelligence analysis initiatives in neglected areas.
- Establish an IC system of data storage, retrieval, and recording of all analysis products and supporting data bases, libraries, etc. These central files, of course, should be made available to all intelligence production units throughout the IC, relieving them of maintaining duplicative and inevitably contradictory data bases and libraries.

By playing this role, the NIC can become the DCI's instrument for managing intelligence analysis throughout the IC. And its acceptance in this role by all parts of the IC will depend on the NIC's clear separation from CIA because other parts of the IC will seldom acknowledge CIA's authority to become directly involved with their work.

3. Separate the Directorate of Intelligence from CIA and subordinate it to the DCI through the NIC. Greatly reduce the DI in size and the areas of intelligence analysis it performs. Make it the DCI's personal analysis arm for selected analysis to fill gaps, highlight anticipated problems, and stimulate follow-up analyses in other IC production components.

The DI has become too large and bureaucratic to perform innovative and insightful analysis. This is not its only problem. Two others are equally serious.

First, because the DI is not located as within DoD or State, the command/management lines of these departments cannot "order" it to do anything. The DI is essentially free to do what it pleases. Military commanders and policy-makers in DoD and State, therefore, have never tried to depend primarily on DI analysis. They may occasionally find some of its products useful, but in their needs for day-to-day and even long-term intelligence production, they depend on their internal, organic analysis capabilities. DI analysts have long been encouraged to get out and "market" their products, and they have tried. For the most part these efforts are doomed before they began because of the very nature of the DI's organizational independence. Not surprisingly, DI analysts have expressed great frustration at seeing their products have little impact on policy. Management techniques by the DI will not overcome these difficulties. They are inherent to organizational structure. There is simply no way to provide "one stop" intelligence analysis support to all departments and agencies needing such products. Yet the illusion has long been sustained in the DI that it is effectively the "one stop," or single source, of valid intelligence analysis support. The analogy with changes in computers is again instructive: once micro-processors hit the market, large mainframe central processors began to decline in utility. The DI has tried to be the "central processor" for intelligence production while "distributed processing" has taken the lion's share of the market.

The second problem is that the DI is spread too thin. It has efforts in virtually all areas of intelligence analysis—general military, technical military, science and technology, economics, political, CI, and so forth. Yet it is not "comprehensive" in any of these areas. For example, the DI does analysis of foreign tanks. No U.S. Army tank development program, however, could survive on the DI's tank analysis. The DI's work is simply too eclectic, incomplete, or untimely. The same is true for intelligence support to any Navy or Air

Force weapons program. In matters of the services' development of military doctrine, the DI's products on foreign militaries would not even begin to provide sufficient information to satisfy their needs.

In economic intelligence, the DI's products are no less inadequate. The amount and variety of economic information gathering and analysis in both private and government institutions is vast. The DI has no prospects for competing with them or for providing significant "value added" analysis. When the Special Trade Representative, Treasury, State, or Commerce officials are engaged in economic negotiations, the IC can supply very helpful support, but most of it is raw intelligence analyzed directly by the negotiators and their staffs. DI analysts are seldom in the loop except when they are detached from the DI and posted on the negotiators' staffs.

Political analysis by the DI generally has the same shortcomings as military and economic analysis. Organic intelligence analysis units in the departments and agencies are better placed to make such analysis relevant, and overt sources—the media, scholarly journals, etc.—are more quickly available and normally better.

The solution to all three of these problems is to change the very purpose of the DI. It should not try to provide "one stop" support to all users of intelligence analysis. It should recognize the age of "distributed processing." Figure 2 illustrates this "distributed processing," showing the main intelligence producers located with the users of the intelligence. Nor should the DI try to compete with the military service intelligence analysts on military topics or with other agencies on economic and political topics. Rather it should be scaled back in size rather dramatically and converted to a flexible analysis unit that looks for problems and issue areas being neglected by other IC components, develops them for the DCI, and then passes them off to appropriate IC components for sustained and comprehensive analysis if that appears necessary. It should not try to "compete" with the rest of the IC in analysis but rather range across all areas, taking a longer view, a more innovative view, probing and pushing in neglected fields to determine if indeed they deserve comprehensive attention. Where the answer is yes, then the DCI can use such exploratory analysis to persuade and encourage one or more IC components to take responsibility for continuing analysis. If the White House and the NSC staff are concerned about areas not well addressed by the NIC and other intelligence production units, the DCI can use the much smaller and higher quality unit to address them.

Because some areas of analysis require diverse and highly specialized skills, this much smaller DI should not attempt to maintain them all within its staff. It should be provided with funds to contract outside research on a temporary, task-by-task basis when its staff skills are inadequate. Through this mechanism, it should give the DCI access to the rich and diverse set of university and think-tank centers with great expertise in particular areas. Most political and economic issues need little or no classified material for first-rate analysis, and for this reason, virtually all of this work should be done on an unclassified basis.

The DI, with this set of changes, would provide the DCI with the means for selected intelligence support to the White House and key departments and agencies without causing disruptive competition between the DI and other analysis units (e.g., within DIA, the military services, INR, etc.). It would provide some depth under the NIC as well, giving it support beyond the IC components, to deal with issues that are not routine, not well accepted within IC analysis circles, or otherwise not effectively addressed.

4. Restructure the Community Management Staff to facilitate the DCI's exercise of his responsibilities for collection evaluation, resource management, and IC policy.

The effectiveness of the CMS, a late comer in IC organizational evolution, has varied with the management style of each DCI. Some DCIs have tried to use it fairly vigorously; others have worked around it or ignored it. The first approach requires that the DCI put significant emphasis on his role as head of the entire IC, standing above and to some degree apart from his role as the Director of the CIA. When the DCI has fallen back on the CIA for his primary staff support, trying to manage the IC as the Director of CIA, the CMS has been extremely weak.

The various intelligence agencies in the IC have been consistently ambivalent toward the CMS. On the one hand, because some of them need national collection management guidance to prioritize their own resources and operations effectively, they see the CMS in a positive light. On the other hand, when the CMS has tried to get into management issues inside the various agencies, they have viewed the CMS as a bother, a troublesome thing to be passively resisted.

The consequence of these ambivalences, on the part of the DCI and members of the IC, has been the emergence of a very large CMS without a clear and sustained mandate (except in a few areas), staffed largely by personnel drawn from various parts of the IC, making it more a representative "parliament" for the IC than a genuine staff. The following structure and functions for the CMS can remedy most of these deficiencies:

- Retain the position of a head of the CMS at the level of a lieutenant general/vice admiral/senior executive service grade 6.

This job is essentially that of a "chief of staff," the person who directs the CMS's work, ensures that its work is fully coordinated, timely, and relevant to the DCI's needs for decision-making. The CMS cannot and should not "give orders" to the IC. Its purpose is to develop decision options for the DCI, analyze them in depth, and to present them with fully developed pros and cons to the DCI for his decision. While the CMS must seek to ensure the DCI's awareness of dissenting views from all IC components, its job is not to resolve disputes or to work out only full-consensus alternatives. The CMS must derive its authority among the IC components from the high quality of its staff work, its consistent openness to factual information, and its innovative development of solutions and recommendations. If it becomes the prisoner of "parochial" analysis and bureaucratic paralysis, it has failed.

- Create five primary CMS staff sections:
 - A) Evaluation Management;
 - B) Resource Management;
 - C) Science and Technology;
 - D) Counterintelligence Management;
 - E) Security Policy.

A) The Evaluation Management Section. This section would be responsible for evaluating the responsiveness of collection agencies to the “national requirements” lists compiled by the NIC from all user departments and agencies government-wide.

Traditionally, the CMS has been responsible *both* for compiling the “national requirements” lists *and* for evaluating how well collectors in HUMINT, IMINT, SIGINT, and other special areas such as MASINT have met them. As noted above, this study calls for the task of compiling national requirements, prioritizing them, and issuing them for the DCI as directives to collection agencies, to be moved to the NIC. Such requirements lists have been standardized for many years, and they are an essential mechanism for all federal departments and agencies to register their long-term intelligence needs and priorities. Collection agencies in the IC need them for annual and five-year planning and programming for their activities.

The second task, evaluating collectors’ responsiveness to the national requirements lists, should remain with the CMS. Much greater emphasis needs to be placed on “evaluation” of collection responsiveness by HUMINT, IMINT, and SIGINT agencies. This can provide the DCI with much better information about the IC’s “outputs,” very important for making decisions about “inputs.”

The CMS evaluation management staff section, therefore, must have sufficient staff to take this responsibility more seriously than has traditionally been the case. And it needs to expand its evaluation efforts to include questioning the agencies making requirements requests to determine if such intelligence is actually needed and used. There is considerable room for innovation in ways that the evaluation process is conducted. Users normally ask for everything although they do not always need it or use it. And collectors sometimes put requirements in the “too hard” box and ignore them.

The evaluation management staff section must also maintain close liaison with the new Collection Management section created in the NIC. The latter obviously is well placed to report on both collection responsiveness and actual needs for the information. And the former, by pressing for such information, can help make the NIC’s collection managers sensitive to priorities and results. In the current arrangement, the CMS can compile the national requirements lists and neglect evaluation. And the NIC and DI are often frustrated about collection management priorities. The change in responsibilities leaves the CMS no option but to deal with evaluation—something much more important for other CMS functions—while giving the NIC control of collection management—something of key relevance to its other duties.

B) The Resource Management Section. This section of the CMS must handle the IC planning, programming, and budgeting process. The budgeting part of this process is well established under Congressional direction, OMB guidance, and so forth. All of that must be retained. What the present system cannot handle effectively is determining the relationship between resource inputs and intelligence collection and analysis outputs. This is simply to say that the present system handles the “line item” budget process as required by the law, but does not impose a PPBS (Planning, Programming, Budgeting System) over the line item program. The major reason for its failure to do this is found in the lack of unified budgets for each of the collection disciplines—HUMINT, IMINT, and SIGINT.

Foreshadowing the sections of each collection discipline, it is necessary here to explain why national managers for each collection discipline are needed with complete program control over resources for their disciplines.

The director of NSA is as close to a “national manager” of a collection discipline as the IC now has. Yet about 40% of the total budget for SIGINT is outside his program control, most in the hands of the National Reconnaissance Office. Despite the creation of NIMA, a large part of the resources for IMINT are managed by the NRO and elsewhere. HUMINT has no national manager, for, although the CIA Deputy Director for Operations (DDO) has control over most program resources for HUMINT and total control over clandestine HUMINT operations, it has been ineffectively exercised over DoD clandestine HUMINT operations.

The obvious and easy solution to this predicament is to designate the Directors of NSA and NIMA the national managers for SIGINT and IMINT (including mapping) respectively, and to make the DDO the national manager for HUMINT. Each national manager, of course, would have his own organization for staff support in executing the national manager responsibilities. Foremost, for resource management, they would include responsibility for demonstrating to the DCI and his CMS the relation between the input of resources and output of collection results in their respective disciplines.

To execute such responsibility, the SIGINT and IMINT national managers must have program responsibility for space collection systems. That is now exercised by the director of the NRO. The NRO, of course, is primarily an R&D and procurement agency with several program offices for contracting with private vendors in the aerospace industry. The NRO should receive its funding from NSA and NIMA, rather than directly from Congress. The NRO itself consists only of a very small staff. Its “program” offices are quite large, consisting of contracting officers and technicians who deal directly with vendors and overseeing their work. All procurement of SIGINT space systems should be put under the management of the Director of NSA. All procurement of IMINT and mapping space systems should be put under the Director of NIMA. These steps would effectively consolidate the SIGINT and IMINT budgets under single-discipline national managers who would be in a position to establish input-output relations in a PPBS fashion to present to the DCI through the CMS for his program review and decisions.

Only such an arrangement will allow a reasonably detached assessment of the mix of space-based and ground, air, and sea-based collection assets for something approaching an optimum mix—or a “satisficing” (satisfactory and sufficient) mix, to use Herbert Simon’s concept of decision-making when the criteria for a truly optimum solution are not available. And they never are in the case of SIGINT and IMINT. Under the current system, however, where the NRO has an independent program which, despite recent public statements to the contrary [2], it is unable if not unwilling to coordinate effectively with NSA or NIMA, even a “satisficing” approach is impossible.

The national manager for HUMINT should have complete program control over all DoD clandestine resources as well as those of the CIA/DO. Overt HUMINT resources are a much larger challenge to manage, but the national manager for HUMINT needs to improve the present situation. He would be responsible for such things as the Foreign Broadcast Information System, for all defector debriefing units, and a number of other assets.

A consolidated Counterintelligence (CI) program with a national manager is also necessary. He must not only oversee the FBI CI budget and the CIA/DO CI budget but also those of the military services.

With these changes in structure of the IC and the designation of national managers for SIGINT, IMINT, HUMINT, Analysis and Production (the NIC), and CI, the Resource Management Section of the CMS would be in a position to present the DCI with genuine alternative program options based on a PPBS approach. With the current IC structure, that is impossible. No issue is more critical for an effective improvement of the IC than this structural problem because it concerns vastly greater financial outlays than any other issue.

C) The Science and Technology Section. This CMS section should be small and staffed by no more than a dozen of the best scientific and technical people available in the IC. Outside scientists should also be brought in for one to three years' service in fields of special importance.

The first responsibility of this section is to stay abreast of all the leading-edge scientific and technological developments in the world that could possibly relate to intelligence collection potential. The second responsibility is to stay aware of all the R&D in every component of the IC and the DoD, DoE, and any other agencies with highly advanced R&D.

Based on information from both kinds of investigations, this section must make recommendations to the DCI for preventing duplications, hiding and non-sharing of R&D where it could be productively shared. This has always been a serious problem both in the IC and in the DoD, and it will probably never be fully solved. Even program offices within the NRO refuse to share technologies. The same is true in other IC components. A small and highly competent CMS S&T section, however, could reduce the number of these cases, especially if it had the DCI's backing and attention.

This S&T section can also play another important role. As was pointed out in the "principles and concepts" section of this study, occasionally the technical collection agencies become so deeply committed to particular technologies and approaches that they are adverse to shifting R&D investments to newer or very different approaches. The S&T Section, when it finds such a situation, could attempt to persuade the agency to invest in different technical approaches. If it resists, the DCI could authorize the S&T Section to contract with a private sector "skunk works" for a "proof of principle" program in order to determine the validity of its judgment about a new technology. If it is successful, then it could be passed on to the relevant IC component and the skunk works closed. Funding for such experimental R&D should come with a strict "sunset" condition. Otherwise, the S&T Section could soon develop its own bureaucratic interest in such programs, pursuing them beyond any practical promise of successful outcomes.

This mechanism for preventing stagnation in R&D and willingness to take high risks in R&D investment is the antidote to the argument that the perpetuation of the NRO is the only answer to the problem. It was originally an effective answer, but it has since become infected with the disease it was invented to prevent.

D) The CI Management Section. This section must keep the DCI abreast of the health of all CI efforts and provide policy recommendations to the DCI for periodic improvements or needed changes. Among the problems it must face is maintaining adequate interagency CI awareness, helping the DCI overcome the inherently parochial and mutually suspicious climate that affects any CI organization. Another challenge

concerns bringing a “multi-discipline” approach to CI, that is, using not just HUMINT collection but also exploiting SIGINT, IMINT, and other technical means in support of CI collection. Finally, if CI organizations remain unconsolidated and fragmented, as they now are, among the FBI, CIA, and the military services, this section will have to devote serious attention to balancing resources among them, that is, helping the national manager.

E) The Security Policy Section. Clearance procedures and the granting of clearances vary widely in the IC and the government. This section must work on steps to reduce the differences and the added costs wherever possible.

It must advise the DCI on security policies for the IC. In this regard, information security, to include computers and communications, is a huge new challenge. While the main concern must be on security in the IC, this section must stay abreast of all of the work in DoD devoted to the defensive side of information warfare. And it may find a role in advising on the kinds of intelligence analysis needed for both defense and offense in the information warfare area to the wider national security community beyond the IC.

These five Community Management Staff sections will probably need to be supplemented with an administrative section for CMS housekeeping, but for the main staff responsibilities, they should be adequate to provide the DCI with the kind of information and analysis he needs to manage collection, resources, and IC policy issues. Most important, they will allow the DCI to introduce PPBS more effectively in relating IC inputs to its outputs.

5. Retain the National Foreign Intelligence Board (NFIB) and the IC/EXCOM.

As noted earlier, the DCI must foster “community” within the IC. The NFIB and the IC/EXCOM are appropriate mechanisms for achieving this climate among the top leaders of the IC.

The NFIB. It has established a rather positive reputation for coordinating agreement and recording disagreement in national intelligence estimates (NIEs) and other national intelligence products. The utility of such products for policy-making is not great, and they have become the focus of a lot of criticism and dispute, especially within the Congressional oversight committees. Still, the NIEs provide DCI-validated statements of intelligence judgments on key issues which are sometimes useful in DoD and State papers when an occasional DCI position is needed. In the JCS, for example, they sometimes provide the language for planning documents.

At the same time, NIEs play another, probably more important, role. The working groups under leadership of the National Intelligence Officers (NIOs), which produce the NIEs, have representatives from virtually all interested analysis units in the IC. They have to meet and consider jointly the available collected intelligence relevant to the questions to be answered in an NIE. This process forces analysts throughout the IC to deal with a common evidentiary base. If there were no such process, over time, different analysts would find themselves working from different sets of evidence, not always sharing or being aware of some evidence. Within IC analyst circles, therefore, the NIE process has the healthy effect of making them communicate and share evidence. If the NIEs performed no other service, they would still be entirely worth the effort.

The IC/EXCOM. The IC/EXCOM, like its predecessor, the NFIC, has never been effective largely because it was intended to deal with resource input-output relations. Only the Director of NSA among its members was even close to having sufficient technical information to be able to speak knowledgeably about the output consequences of alternative inputs of resources. Yet he was limited to solid knowledge of only a little more than half of the budget for SIGINT. The Director of NRO has no basis at all for understanding input-output relations in any of the disciplines. His logical and imperative role has always been to defend a growing NRO budget without regard to its impact on the overall collection capabilities of the IC. The Director of DIA is little better positioned to comment on all but a few resource issues. The same has been true for all other IC/EXCOM members. Not surprisingly the IC/EXCOM has failed to establish itself with the DCI as useful forum.

Reconstituted, this would change. With national managers of the collection disciplines, analysis, and CI in its membership, the IC/EXCOM would be able to give informed advice to the DCI on budgetary and policy matters. Moreover, if the CMS were reconstituted as recommended above, it would be able to present the IC/EXCOM with meaningful options and supporting analysis.

IC/EXCOM discussion in such circumstances could be enormously productive for the DCI and the IC top leadership as well. As the DCI became more assertive in exercising his management role, the IC/EXCOM would be extremely helpful to him by providing the IC leaders a forum for expressing advice, consent, and dissent. They could not complain, as they so often have, that they were excluded, that CIA alone was dictating IC decisions, or that the DCI was making his decisions on the basis of highly uninformed or patently parochial analysis.

6. Require the DCI to conduct a structural review of the IC every five years to ensure that its organization is keeping abreast of needs for change of two types: a) new technology and b) growing dysfunctions caused by inherent organizational behavior.

Most of the needed changes in the IC today arise from changing technology and the current IC structures' limits to exploiting it fully. Some also are due to inherent organizational behavior that creates dysfunctions not foreseen several decades ago. The IC must deal with a dynamic world in two regards. First, as a developer and user of leading edge technology, it confronts steady and relentless change. Second, as an intelligence organization, it confronts a world of varying and changing targets. To cope with both dynamics, it has to adapt, sometimes rapidly. Fifty years old in 1997, the IC has, of course, adapted its structures occasionally—the creation of the NSA, NRO, DIA, and CMS are examples. But over the last three decades, with the exception of NIMA's creation in 1996, no significant structural changes, however, have been implemented. Yet this period has witnessed the most dramatic technological change. At the same time, the IC's largest customer, the Department of Defense, has experienced equally dramatic change, both due to new technology and to changing force structure and regional missions. The Department of State, also a major user of intelligence, has experienced significant changes itself. Treasury, Commerce, Energy, and other departments have become bigger users of intelligence with changing demands.

The IC, therefore, should not have to wait on a major crisis to stimulate reform and structural change. Adaptation might as well be built in as a periodic requirement. This is not to endorse change for change's sake or to make a fetish of it. Organizational reform can be very wrong-headed, disruptive, and even

regressive. This point deserves some clarification because the plethora of studies calling for IC reform today is disorienting. Which make sense and which should we treat skeptically?

An example of a misguided rationale for IC reform is that the end of the Cold War demands it. That is not at all obvious. The dissolution of the Soviet Union certainly changes the targets for the IC and demands a new prioritization. If the IC's structure was already highly effective in use of resources, and if it were adapted to exploit the technologies it has deployed over the last two or three decades, there would be no case for IC reform, the emergence of many different intelligence requirements—e.g., drug-trafficking, nuclear proliferation, new forms of terrorism—notwithstanding. In that case, the IC would only need different “collection management” direction. Its collection agencies and production units would respond appropriately. The new set of output requirements might demand adjustments with the IC components, personnel with different language skills and area knowledge, new sites, new data bases, etc. These changes, however, would require no structural reform of the IC, only a somewhat greater shift in resources than happens normally from year to year in the resource management cycle.

To use a metaphor, if one has a passenger airplane that flies regularly between city X and city Y, and if all the passenger demand dries up on city Y while demand in city Z is growing, all that is required is a shift in the airplane's schedule, responding to the demand in city Z and cutting trips to city Y. No one would recommend that a basically different airplane is needed to make the shift. On the other hand, if the airplane's fuel consumption had been rising, its maintenance costs going up, and its avionics were increasingly obsolete, a new and different airplane would certainly have to be considered. The IC today is closer to the latter situation than the former. Reform requirements are not a function of a changed flight route but rather of overdue maintenance, changing avionics, engine efficiency, and other such structural issues.

Another kind of misguided approach to reform arises from excessive concern with technology at the expense of organizational realities. A particular example is worth citing because some critics of this study will inevitably raise it. The technologists have long been fascinated with what is called “cross-cueing,” that is, using data collected by either SIGINT or MINT to “cue” the collection of the other discipline. This concept makes very good sense, and it is widely applied even within the present IC structure. The technologists, however, are not satisfied with cross-cueing done by collection managers of two different disciplines talking to each other and cueing each other by organizational routines. Instead, they want to “automate” the process, to link up SIGINT and IMINT capabilities with “software” applications that do the job without much human intervention.

In principle, the idea sounds attractive, and *a priori* one cannot reject it. But any serious *a posteriori* understanding of the current organizational realities and the complexities of processing both SIGINT and IMINT from advanced systems makes the idea downright ridiculous for the foreseeable future. No doubt, a stand-alone SIGINT system, narrowly focused on a particular kind of target, could be coupled through computers with a stand-alone, narrowly focused IMINT system and made to cross-cue each other against an equally narrow set of targets. It could most likely be made to work if an autonomous organization were created and dedicated to it.

But does it make sense? Suppose the target set suddenly loses its importance? Like city Y's loss of passenger traffic in the example just cited. The IC would be left with the equivalent of an airplane which could only fly to one city! More likely, the owners of the target set will soon become aware of the system and they will devise ways to spoof it or mislead it with changed signatures. Absolutely certain to happen is that the new organization created to make the system work will develop a bureaucratic life of its own, squandering resources long after its fecklessness is established beyond a reasonable doubt. A number of TIARA programs stand as painful and expensive evidence of the wrong-headedness of letting cross-cueing technology ideas get ahead of organizational capacities and ignore the target realities. Several versions of "tactical ELINT processors" are examples. The Navy has stumbled on some of them but has largely adjusted by putting more humans in the loop, taking them back toward more traditional "manual" checking of cross-cueing. The Air Force's B-1 bomber program finally had to give up such automated, multiple-source processing—with no human intervention—on board the aircraft. And the Army's relentless pursuit of the impossible in the Joint Tactical Fusion Program still limps along.

The lessons here are not that technology does not sometimes demand organizational change, or that technology solutions may not surprise us with their effectiveness at times, or that high initial costs ought to kill high risk R&D. The lessons are different. First, organizational reform has to catch up with the technologies already fielded and working well, especially when it is reasonably clear that such reform promises considerably improved efficiency in resource use and in performance. Second, the venturesome technologists, if their innovations are constantly pressed against target realities and organizational implications, will push organization into highly dysfunctional forms, if not at once, then in the near future. Third, some technology schemes, feasible though they are, simply do not have significant real-world applicability.

For actual cases of all three lessons, one only has to look at the last two decades of experience with applying computers, advanced communications, and networking systems to organizations of all sorts. Many initial promises have failed. The sales hype is misleading as often as not. Great gains in "factor productivity" are eventually made but not always the ones predicted. The "information superhighway" rhetoric certainly will not materialize in fact. The print media, contrary to predictions, have not disappeared. Nor have libraries with paper books. Nor has automation created many "paperless" offices.

The economic marketplace forces most of these wrong-headed concepts to be abandoned sooner or later. In the IC, where no market mechanism exists to expose such fallacies, the sensible alternative is a healthy degree of skepticism coupled with periodic organizational reviews and reforms.

Conclusion

In some regards, these recommendations for the DCI's management structure involve major changes, not only in his staff support but also within the components of the IC itself. On the other hand, they merely involve improvements in long-existing institutions that have emerged in an evolutionary manner.

The evolution process, however, has long ago come up against rigid structural problems within the IC that block its logical and effective continuation. Two major ones stand out as examples: the role of the NRO and the place of the CIA/DI.

The NRO made sense when it was created. Using space for technical collections systems was far beyond what NSA could have managed in the 1950s and early 1960s, and no IC component at the time was capable of the vision and risks that were required to create imaging systems in space. Moreover, the regular R&D and procurement system would probably have stifled the entire space intelligence program. Thus the creation of a separate agency, dedicated entirely to high-risk R&D and systems procurement and staffed by imaginative leaders, proved itself. At the same time, there was no way to anticipate the constellation of different space systems that would eventually be fielded. By the late 1970s, however, great progress had been made, and a complex array of systems were actually operating in space. The need for innovation at this point was not mainly in R&D for more advanced systems. It was in techniques of operations which could combine the different space systems with earth-based collection systems, and which could rapidly redirect them to deal with crises and to make them effective in support of tactical military operations. NSA made progress in these areas although against strong bureaucratic resistance from the NRO and also from several of its own internal subunits. The military services also proved obstructive in some regards, and in the case of the Navy, it tried to build its own dedicated space intelligence system. When U.S. Space Command was created in the 1980s, it asserted itself in the IC, seeking at times to take control of some of these systems without understanding the way NSA was using them to support the Space Command and without the vaguest idea of how it would employ them if it had control.

The second example, the CIA/DI, goes back to the creation of the IC by the National Security Act of 1947. The CIA was to have an analysis unit primarily for strategic and tactical warning that was lacking in 1941 before the Japanese attack on Pearl Harbor. The Army and Navy intelligence systems had failed; thus it was believed essential that a national-level "central" analysis agency be created. As the NRO fielded space systems and NSA expanded its world-wide collection system by the 1960s, an entirely different approach to intelligence warning became imperative. The White House Situation Room was created after the Cuban Missile Crisis revealed the serious lack of communications connectivity among the national security departments on command centers. The resulting network of communications and the warning system of "critics," managed by NSA, linked the current intelligence staffs of the military services, State, and several others with the White House. The speed with which warning intelligence was generated by this system largely shunted the DI aside.

As U.S.-Soviet arms control negotiations began in the late 1960s, the DI grabbed a central role in supporting them, one that created serious friction with the military services' intelligence analysis units, involved CIA in only an eclectic fashion in military intelligence production, and tended to interfere with military intelligence support for weapons modernization and doctrinal development. With the reduced importance of arms control negotiations resulting from the end of the Soviet Union, the DI has scrambled for missions, engaging in eclectic production of military, economic, and political intelligence without serious consumer demand, and building a legacy of bitter disputes with DIA and the military service intelligence organizations. The DI had become too big and bureaucratic to provide the kind of intelligence the DCI could best use, and it was wholly ill-disposed and ill-staffed to help him manage a cooperative allocation of intelligence production

responsibilities among all the IC analysis organizations. In this predicament, it has wound up defending itself against charges that it failed to predict the end of the Soviet Union (a nonsense debate) and inventing ideas about providing economic intelligence to American business and other such dubious schemes.

There are other IC structural problems, but these two examples are sufficient to show that, like any major organization or business activity in a world of rapidly changing markets and technology, the IC structure that once worked effectively became increasingly dysfunctional. Fundamental change is long overdue.

This critique of the present situation and the recommended changes would not only remove the blockage but advance the evolutionary process to catch up with two decades of stagnation. They would remove structural “turf” problems that squander IC energies in struggles that weaken the DCI as the leader of the entire IC. And they would provide the DCI with the mechanisms and processes necessary to assert strong leadership over the IC.

Notes

1. This informal “concurrent” authority of the DCI over high-level appointments has recently been formalized in law in the case of the appointments of the directors of NSA, NIMA, and NRO. The DCI is also to be “consulted” in the case of the appointments of the Director of DIA, the Assistant Secretary of State for Intelligence and Research, and the Director of the Office of Nonproliferation and National Security of the Department of Energy. Public Law 104-293—Oct. 11, 1996, section 815.

2. See prepared testimony of Keith Hall, Director of NRO, before the Senate Armed Services Committee, March 12, 1997, p. 3.

Section IV

The Defense Department's Intelligence Structure: A Review and Recommendation for Reform

Introduction

This section focuses on the intelligence organizational structure and links within the Defense Department (DoD) above the services and unified commands. Detailed attention to the intelligence structures of the military services and the unified and specified commands is beyond this review. The reasons are the same as the ones guiding the overall study of the IC. The review is a top-down management and structure critique. It aims neither to provide solutions to all IC problems nor an excessively small-grain look at structural issues. Rather it seeks to understand how a few key structural and management changes at the top levels in DoD intelligence can be made that would provide a more effective allocation of responsibilities and missions. With that rationalization of the top management structure, incumbent senior intelligence officers would have a much improved prospect for continuing the rationalization down the intelligence command levels into the military services and the unified commands. In other words, improving things at the top is the first order of business and also about all that can be done in the initial phases of a DoD intelligence reform. If that is done well, the reform is likely to be continued downward over time.

Some discussion will involve selected aspects of both the military intelligence organizations and intelligence operations in the forces deployed under unified commands. This is necessary because the intelligence organizations in the Pentagon are linked to them in many ways. An understanding of DoD intelligence, therefore, requires an appreciation of several of those linkages.

It must also be emphasized that the guiding concepts for conclusions and recommendations in this section, like all the others, come from the study's section on intelligence doctrine and principles for resource management. The recommendations offered are meant to bring both organization and process into line with the doctrine and management principles.

As a general outline, the review first treats DoD intelligence organization and processes for providing intelligence support, that is, the way they work for providing "outputs" of intelligence. Then it examines the system of resource management, the "inputs" of money and personnel for DoD intelligence. In dealing with both aspects, intelligence support and program management of resources, excursions beyond the confines of the Pentagon are essential because those organizations and processes inside the Pentagon are inextricably tied to the larger IC and to the military services and unified commands. Finally, the review makes a series of recommendations.

The Present DoD Intelligence Structure for Intelligence Support

DoD intelligence organization is complex. That is apparent from a look at the Defense Intelligence Agency's table of organization (Figure 3). Complexity is also evident from a look at the formal and informal role of the Assistant Secretary of Defense for C3I (Command, Control, Communications, and Intelligence). Similarly, the same picture emerges from a look at the disposition of CI responsibilities. The Joint Staff under the Chairman of the JCS has not traditionally had a full J-2 as the primary staff officer for intelligence, but a DIA element, dedicated to the Joint Staff and headed by a flag officer, effectively plays that role. The military intelligence representation within the Pentagon is less confusing. As one would expect, each military service staff has a primary staff officer for intelligence. The best way to sort out this maze is to begin with understanding how the military service intelligence chiefs and their organizations link to DoD intelligence. In the process, the primary kind of intelligence support that the military services need is explained. That clarifies part of the DIA's relationship to the military services. Next, we look at the system of intelligence support to current operations in the Joint Staff and in the operational forces in the unified and specified commands. Finally, a number of other intelligence elements and officials in DoD are examined [1]. That will provide a general picture of the present organization, roles, and processes.

The Role of Military Service Intelligence Organizations and their Relation to DIA

The military services' intelligence organizations are represented in the Pentagon by the principal, or senior, intelligence staff officers of each military department, specifically, the Army Deputy Chief of Staff for Intelligence (DCSINT), the Air Force Assistant Chief of Staff for Intelligence (ACS/I), the Navy Director of Naval Intelligence (DNI), and the Marine Corps Director of Intelligence (DirInt). They are effectively the service intelligence chiefs. They, of course, have support staffs to assist them in handling their services' intelligence issues for both joint and service policy-making. They also participate as members of the Military Intelligence Board (MIB), chaired by the director of DIA. Likewise, they also participate in the NFIB, and their representatives are found on most CMS committees. Thus the service intelligence chiefs stand as the primary management and policy-making link that the DCI and the director of DIA have with the services' intelligence organizations and capabilities.

In noting the place of the military service intelligence chiefs in both DoD intelligence and the IC, it is also important to emphasize in general terms what the military service intelligence organizations do. Their lower-level tactical intelligence units organic to combat units deployed under the unified and specified commands are dedicated to providing support to military operations. Each military service has to recruit, train, organize, equip, and field these units. The military intelligence chiefs are not the primary staff officers responsible for these force development tasks. The force structure and program staff sections, again, not the service intelligence chiefs, of the military department staffs manage these tactical intelligence organizations and collection systems. This is important to note because it shows why the Military Intelligence Board (MIB), composed of the Director of DIA, the service intelligence chiefs, and several agency directors has no program management responsibility over tactical

intelligence forces and systems (i.e., the TIARA aggregation). That responsibility gets lumped into the same staff sections that handle each service's procurement programs and force development issues [2].

The service intelligence chiefs' most important role concerns intelligence analysis. Although it varies among the services, the service intelligence chief generally has staff supervisory responsibility for the provision of intelligence analysis to support all his service's weapons programs and force development issues. In other words, he oversees the "threat" data against which U.S. weapons and forces are required to perform successfully. The amount and complexity of "threat" data needed to support weapons systems is great indeed. And the impact of variations in assessments in threat data can be enormous where the cost of a program is concerned. Upper-range estimates of "threats" (usually estimates of the technical aspects of foreign weapons systems and defensive measures), by increasing the requirements for U.S. capabilities, may push up the cost of a service's weapons program by dramatic amounts; likewise, lower estimates can reduce it.

Thus intelligence support for materiel and force development to the military services is both a very large task and a factor to which program costs are highly sensitive. This area of intelligence is virtually overlooked in most critiques of the IC and reform proposals. Throughout most of the IC, especially outside the military service intelligence circles, it is not even vaguely understood. At the same time, most of the intelligence collection needed for this kind of "threat" analysis is done outside the military services, mainly by SIGINT and IMINT, supplemented sometimes by HUMINT. The impact on the allocation of large dollar sums caused by this intelligence is real, measurable, and critically important. By comparison with most "national" level intelligence products, its impact on resource allocations is vastly greater. Proving that an NIE or similar product has a real and measurable impact on policy and resource allocations is difficult, and in more cases than not, the impact is nil. Yet congressional attention, DCI focus, and the several recent intelligence reform studies largely ignore the issue of intelligence for materiel and force development in the military services.

How to improve such intelligence and how to make it more effective are beyond this study, but awareness of the impact it has is important. At the same time, the NIC and the CIA/DI are essentially out of this intelligence production loop. The DI's science and technology and general military intelligence analysis sometimes has an influence on it, but for the most part the DI is institutionally disconnected from the materiel and force development processes. The military service intelligence production units and private vendors, performing analysis on contract, are the major providers. These realities provide strong support for the recommendation in the section on the DCI's management structure for reducing the size of the CIA/DI and changing its mission considerably, including elimination of its responsibility for production of regular military intelligence. Such products as it turns out have at most a trivial impact on materiel and force development decisions. If they were not available, they would hardly be missed.

A final point on intelligence for service materiel and force development concerns DIA's contribution to it. DIA is dedicated in principle to such analysis. It is supposed to manage the "threat" data for support to joint weapons programs and several large programs that receive special oversight by the office of the Under Secretary of Defense for Acquisition. DIA also allocates specific S&T intelligence production responsibilities among some of the military S&T production centers and holds approval authority over their products as validated "defense intelligence." In other words, DIA holds considerable formal authority over military

intelligence production to support materiel and force development. To have a DoD-level authority referee the services' efforts in this production and to ensure no duplications in analysis among the military services were reasons invoked by Secretary McNamara when he directed the creation of DIA in the early 1960s.

In conclusion, it should be clear that the military services' main intelligence requirement is for analysis to support materiel and force development. While the services' organic intelligence organizations actually produce most of it, DIA also has a major responsibility for overseeing this production and contributing to it, especially for selected joint and large DoD acquisition programs. It should also be noted that this kind of intelligence support is not very time-urgent. Minutes and hours do not make a difference although weeks and months of delay can adversely affect the schedules for weapons programs. Figure 5 shows intelligence collection and production for material force development, and also for support to military operations, which is discussed below.

DIA and Intelligence Support to the JCS and the Operational Forces

The JCS intelligence support element (roughly the J-2 for the Chairman of the JCS) is supplied by DIA. Thus at the Joint Staff level in the Pentagon, intelligence support—as a staff function—is provided by a DIA component. DoD intelligence is also linked to the unified and specified commands, i.e., the forces deployed under the CINCs with combat contingency responsibilities, primarily through the J-2s (the primary staff officers for intelligence) in those commands. DIA maintains intelligence communication links with the J-2s of the unified commands and some of their intelligence support units. Recalling the doctrine section of this study, it should be remembered that J-2s are analysis and production staff sections. They may be supplemented by dedicated analysis units, but each is a CINC's staff element that directs collection and produces analysis for his planning and conduct of operations, functions done by his J-3 and J-5 staff sections. Each service component within a unified command, however, also has organic collection and production capabilities, and they must be integrated into the command's intelligence system.

Again, recalling the doctrine principle that distinguished between “collection management” in general and “technical collection management,” let us turn to how intelligence collection should, and sometimes does, work for the operational forces. The collection disciplines, of course, are SIGINT, IMINT, HUMINT, and CI. For illustrative purposes, let us take the SIGINT case.

Organic SIGINT collection capabilities are found in some of the military units at the tactical and operational levels. And very large SIGINT capabilities exist at the national level, under NSA's direct operation. At the J-2 level in a unified command, and in the upper naval, air, and ground unit intelligence staff levels in the service components, NSA deploys Cryptologic Support Groups (CSG). A CSG is composed of personnel with expert knowledge in how to task the SIGINT system, directly dealing with NSA's main operational center when necessary and also expert in knowing how to make the most sense of SIGINT products when they are delivered. CSG personnel, however, have neither the competency nor the technical information to direct SIGINT “technical collection management” to obtain desired results. The CSGs depend on NSA to perform that function.

Because NSA has OPCON over the world-wide system, it can, if it desires, redirect relevant parts of the system to support a single local military operation. In the process, however, it often must cease coverage of targets to meet other requirements that the DCI has placed on NSA. In crises and military combat operations, the NSA operations center makes these necessary collection adjustments on a massive scale, bringing to bear a wide array of systems—space-based, aerial, ground, and sea collectors—on the appropriate targets. The degree of technical expertise and diversity of skills required for this kind of collections management is simply beyond what any unified command's J-2 staff can possess. This is also more than the DIA support element with the Joint Staff in the Pentagon can do. Leaving SIGINT "technical" collection management to NSA, therefore, is the only practical alternative. Unfortunately, many military intelligence officers do not understand this reality, and that has caused numerous counterproductive turf battles in the area of SIGINT collection management.

Because of the peculiar nature of the SIGINT discipline, effective use of tactical SIGINT is also frequently better done under the technical direction of NSA and not by the tactical SIGINT unit's technical controllers. There are exceptions, but experienced SIGINT personnel can quickly recognize which is which. J-2s, G-2s, and other tactical-level collection management authorities are wholly unqualified to be involved in this technical affair. Their business is specifying the results from collection that they desire, how soon they need it, and where it is best delivered directly.

This explanation of some of the technical aspects of SIGINT collection are important to emphasize for another reason. CINCs of unified commands and others frequently look at the NSA technical management system as well as other specialized intelligence structures as "stove pipes." "Stove pipe" in this usage has a negative connotation. Stove pipes are considered "bad," and therefore, should be broken down. But nothing could be more wrong when it concerns "technical collection management," and not just management of SIGINT collection. IMINT and HUMINT also require special "technical" collection management when national assets are working in a coordinated fashion with tactical collection assets.

The way to solve the problem of "stove pipes" is not to remove them. It is to make sure that every command level's intelligence staff section knows how to obtain access to the "stove pipe" in order to levy its collection requirements on that collection discipline. The "stove pipe" structure is the very thing that has allowed the SIGINT system to bring national collection assets to bear on tactical collection requirements. This flexibility in making space-based systems and many other systems work for a tactical commander requires not only enormously skilled technicians. It also requires a large and complex communications system. And it requires a diverse set of processing skills which no military unit could maintain, much less employ. The ability to perform this kind of technical management of all kinds of collection systems is so complex that it can only be done at the national level. It was not easy for NSA to develop, and it requires constant effort to maintain it. Without it, the old fissure between tactical collection systems and national and other systems would reappear with all the degradation in SIGINT support that would entail. The system would drop back to the status of the 1970s, giving up all the progress it has made in the 1980s and 1990s. Even with the creation of NIMA, IMINT collection management still has a long way to go. The historical absence of HUMINT and IMINT stovepipes is why field commands, during combat operations, almost always have been dissatisfied with HUMINT and IMINT support.

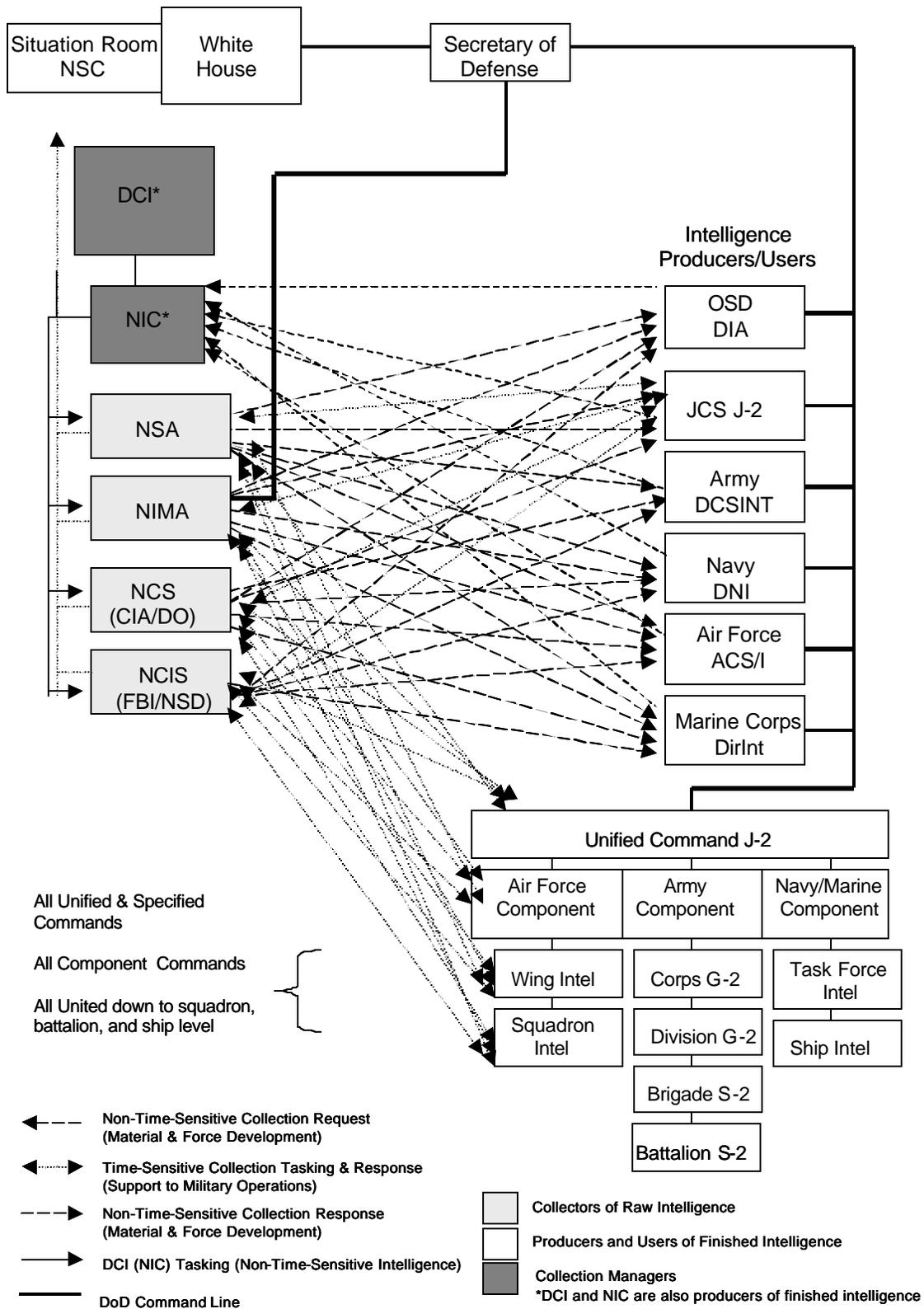


Figure 5. Reformed DoD System of Intelligence Collection and Production for Material and Force Development and Support to Military Operations

The view that all “stove pipes” are dysfunctional is patently wrong. Until commanders and the intelligence staff officers understand the imperative for some kinds of “stove pipes” in intelligence collection, they will be an obstacle to the very intelligence support they desperately seek.

A similar approach to the technical management of IMINT is long overdue. A major task for NIMA will be to create just such a technical collection management “stove pipe,” making it accessible to staff intelligence sections and other users down to the lowest tactical levels. When that is done, the present diverse set of IMINT systems can be concentrated and put to work to support military operations under whatever priority the JCS and the CINCs dictate. NSA is under the direct command of the Secretary of Defense, and NIMA is also. Their directors will readily respond to JCS prioritization of time-urgent intelligence support to military commanders.

HUMINT is greatly different in the nature of “technical control” required for its collectors, but the principle of a national system is the same. CI is much like HUMINT in this regard. The major service it can provide is information about the enemy’s intelligence collection capabilities and their targets. National level information will not be all that useful in many cases, but a well-developed national CI system with coordinating authority over aspects of the military services’ CI assets might prove highly effective.

Military commands have considerable means to collect intelligence beyond the national SIGINT, IMINT, and HUMINT systems. Not only do they have organic specialized intelligence collection assets; they normally use combat forces themselves to collect intelligence. The collection management of these capabilities is the responsibility of the commands themselves. The only exceptions arise when there is a need to coordinate local collection efforts with national efforts, that is, allocating the proper division of tasks between tactical and higher level SIGINT, IMINT, HUMINT, and CI capabilities.

Two points in this review deserve special emphasis. First, the national collection disciplines—SIGINT, IMINT, HUMINT, and CI—can and must be brought to bear in supporting tactical military operations. And that can be done most effectively by acknowledging the highly technical tasks involved and the requirement for certain types of “stove pipes” to be created and maintained.

Second, most intelligence support to military operations (SMO) is time-urgent. Non-urgent intelligence support is also required, especially in peacetime for planning by the Joint Staff and the unified commands, but this has not been the problem area. Current operations are the greater challenge and of primary importance. Time-urgent intelligence support, of course, requires adequate communications. Yet they have been generally lacking in all areas but for SIGINT.

Types of Military Intelligence Support

The foregoing analysis has distinguished consistently between two basic classes of military intelligence support. The first is support to materiel and force development. It is heavily technical in character, but general military intelligence about doctrine, organization, order of battle, and so forth are also critical to it. This type of support is used almost exclusively by the military services and the Office of the Secretary of Defense (OSD) staff concerned with procurement and R&D.

The second type of military intelligence is SMO. It is most often time-urgent, and it concerns the current behavior of foreign governments and militaries. Its users are almost exclusively the JCS and the unified and specified commands.

The importance of the distinction in types of intelligence support is clear when one considers organizational arrangements for analysis and production responsibilities in DoD. The production of intelligence support for materiel and force development, to the degree possible, should be organizationally separated from the production of intelligence support to military operations. They are quite different, requiring different skills in many cases, and the schedule of production for each is dramatically different. The former is more analogous to publishing scholarly journals and books; the latter is more like producing a daily newspaper and TV news coverage. DIA sits astride both responsibilities, and that is a major source of some of its problems. Within the military services' intelligence organizations, a similar overlap is occasionally found. Any serious reform effort, therefore, must look at how these overlaps can be removed and how organizations can be given responsibility primarily for one type of intelligence support.

Counterintelligence Organization

CI organizations and operations in the DoD share no common doctrine of organization and operations. The Army maintains CI units whose mission is purely CI. Army law enforcement belongs to its Criminal Investigation Division (CID), and CID has no CI responsibility. In the Air Force, CI is the responsibility of the Office of Special Investigations (OSI), which is also the Air Force criminal investigations authority. Likewise, the Navy's Naval Investigative Service (NIS) combines CI with its law enforcement function. The operational arms for CI in the services include a large number of units deployed throughout each service's installations and deployed forces.

Within OSD, CI is coordinated by one of the Secretary's staff sections. It has changed over time, from the ASD/I in the 1970s to a deputy undersecretary in the 1980s, and now to the ASD/C3I. The precise meaning of "coordination" has also varied. Working up CI policies for the Secretary of Defense to promulgate, actually getting involved in an occasional complex CI case, and playing some part in overseeing the CI budget have been included in the "coordination" function at different times.

This arrangement leaves military CI essentially headless within DoD. Neither an Assistant Secretary nor a Deputy Under Secretary has "line" management authority, although incumbents have occasionally tried to exercise it. Both are staff officers for the Secretary, not "operators" or "managers." The absence of a line management element at the Joint Staff or OSD level leaves both cooperation and coordination among the services' CI operations as voluntary matters. It also means there is little management capacity to impose uniform standards among the services.

For example, it was noted that the Army alone separates law enforcement from CI. The two do not mix well. The methods for successful CI work are significantly different from criminal law enforcement methods. Good CI work is far more expensive per average case resolved. In part this is because the aim of CI is not just to identify and arrest enemy agents but also to learn about the full extent of an adversary's intelligence

capabilities. That may require lengthy surveillance periods to uncover an agent's network of support, to discover other agents, and to assess the foreign intelligence service's methods and capacities. The tendency of law enforcement agencies, on the other hand, is toward early arrests and prosecution. Law enforcement and CI also do not normally involve the same set of methods for investigation. Truly advanced CI work involves a multi-disciplinary approach in which SIGINT, IMINT, and HUMINT collection are combined. And it tends to involve world-wide connections that are seldom found in military criminal cases. Narcotics and terrorism, of course, are exceptions, but they make the point: law enforcement agencies have not done very well in handling these problems, because the perpetrators have much vaster resources and organization—more like sovereign governments. Moreover, they are sometimes sponsored by states.

More specifically for military CI handled by law enforcement organizations, the NIS handling of the Moscow embassy guard case in the 1980s was seriously bungled in no small part because it was in the hands of law enforcement agents who lacked these quite different CI skills. The case of a retired U.S. Army sergeant (Clyde Lee Conrad, now serving a sentence in a German jail) working for Hungarian intelligence in the early 1980s stands in stark contrast. Law enforcement personnel would never have pursued the case because the initial evidence of a CI problem was extremely vague. Army CI agents required several years to get a clear lead, and they then conducted two years of surveillance, unraveling a number of other agents of hostile intelligence operations, before asking German authorities to make an arrest.

Without a Defense Department management structure over all three military CI organizations, there is no way to get them all up to a similar professional level. Nor is there a way to coordinate joint operations and to share techniques and data in regularized fashion.

Defense Intelligence Collection Capabilities

DIA was created primarily as an intelligence analysis and production organization. Today the center of gravity of its activities remains in analysis and production. As our doctrinal principles assert, analysis and production are distinctly different functions from intelligence collection, and as a rule, it makes sense to keep them organizationally separated. As it is now organized, however, DIA violates that principle because it has a number of collection capabilities (see Figure 3).

First, DIA manages the defense attaché system, a very effective overt HUMINT collection asset. Second, DIA operates the Defense HUMINT service (DHS). Founded in 1995, DHS combines the HUMINT capabilities formerly operated by the military services. Third, DIA has OPCON over a number of aerial reconnaissance programs that involve IMINT and special signals collection. Fourth, DIA has kept a hand in managing ELINT collection and analysis, especially for its JCS support element's warning center. ELINT is the collection of radar signals, actually a branch of SIGINT. Finally, an odd assortment of overt HUMINT collection efforts, e.g. debriefings, interrogation programs, etc., are managed by DIA, and similar capabilities and programs exist in the military services, e.g., the Army's interrogation battalions.

This potpourri of collection efforts ranges from reasonably effective to dubious in value. Given that DIA's major task is analysis and production, the question naturally arises as to whether it needs control over any collection assets.

DoD Personnel Security Programs

Security is not, properly speaking, an intelligence function, but rather a command responsibility. Because security clearances for personnel in all parts of defense intelligence are issued by various security agencies, and because CI operations are concerned with clearances, it is important to note the existence of the Defense Investigative Service (DIS). It is a centralized DoD organization with overall responsibility for clearances within DoD, but the military services have also maintained security clearance systems. Moreover, NSA, the NRO, and a few other agencies have their own security clearance procedures. In part these smaller security clearance activities are survivors from the period before DIS's creation, but they are also a reflection of the low regard for DIS's standards. Its task is huge, and its resources have never been abundant. Whether it could recruit and maintain a truly first-rate work force is an open question. It has improved, but its job is thankless, and it has never had strong support from the top leadership in DoD. Other priorities simply push DIS to the back of the queue of organizations needing attention.

This study will make no recommendations on DIS and other security programs in DoD. The security clearance area, however, deserves serious reform attention.

The Defense Intelligence Resource Management System

Programs and budgets for intelligence in DoD are numerous and somewhat fragmented, although there is a system for aggregation and review to overcome duplications.

NSA has its CCP (Consolidated Cryptologic Program); NIMA has its NIMAP (National Imagery and Mapping Program), and NRO has its NRP (National Reconnaissance Program), part of which comes from the Air Force budget, the other part from CIA. DIA manages the GDIP (General Defense Intelligence Program) which includes a number of elements within the military service intelligence budgets and those of the unified commands, primarily Joint Intelligence Centers (JICs). These are relatively small and do not include tactical intelligence systems. The GDIP, of course, includes all of DIA's component programs. All of these, CCP, NRP, and the GDIP, are part of the DCI's NFIP. He is the senior program manager for the combination of all of them. The CCP and NRP are very large programs, making up the largest share of the NFIP. The GDIP is smaller by comparison.

CI programs come under a separate management structure, being combined within DoD under the Foreign Counterintelligence Program (FCIP) [3] and included in the NFIP with the CI part of the FBI's budget and the CI part of CIA's budget [4].

The sum total of these programs is several billions of dollars. Yet they do not include all of the intelligence programs in DoD. A large set of tactical intelligence programs exists, involving some that are merely

“related” to intelligence. For example, a standard aircraft, which may serve non-intelligence purposes as well but carries intelligence collections systems, would be a “related” program cost. Support personnel for maintenance and other non-intelligence personnel supporting tactical intelligence systems are considered “related” costs to tactical intelligence programs. At the OSD level, all of these are combined under the TIARA (Tactical Intelligence and Related Activities) aggregation. TIARA includes funding for tactical SIGINT systems. And it contains a number of imagery and other programs.

The TIARA budgetary aggregation is quite large, well over \$10 billion. It was constructed at the request of the Congress in order to provide an idea of just how much is actually allocated to intelligence outside the NFIP. Drawing the line between what rightly deserves to be included and what should be excluded is not easy. For example, some target acquisition systems are so entangled with weapons systems that one can argue cogently against their identification as TIARA programs.

In 1994, a new intelligence budgetary program was established, the Joint Military Intelligence Program. The JMIP is to include DoD programs involving resources of more than one DoD component, when users of resulting intelligence are from more than one component, and/or when centralized planning, management, coordination, or oversight will contribute to the effectiveness of the efforts. The JMIP was established by transferring a number of TIARA programs [5]; U-2 surveillance aircraft, which had been funded out of the NFIP, have also been added [6].

At the level of OSD, the ASD/C3I has staff oversight responsibility for all DoD intelligence programs, those in the NFIP, JMIP and TIARA. At the same time, this ASD is not really a “program manager.” He is primarily the Secretary of the Defense’s eyes and policy advisor on intelligence programs. His inclination, however, is to try to assert program management control in the absence of a line program management authority over TIARA.

The reasons are easy to understand. First, the ASD/C3I receives pressure from Congress to improve the management of TIARA. Second, he is in a position to see the functional fragmentation, especially between NFIP SIGINT elements, such as the Consolidated Cryptologic Program, the Defense Cryptologic Program in the JMIP, and tactical SIGINT programs in the TIARA aggregation. Getting the military services to cooperate and avoid overlap in R&D and procurement of tactical cryptologic items is difficult, and making tactical SIGINT capabilities fit with the CCP and DCP capabilities is even harder. In coping with the latter challenge, the Director of NSA helps him, but even NSA is limited in its influence with the military services on many tactical SIGINT issues. The disconnects between NRO programs and the CCP have already been discussed, and similar disconnects between the NRO’s IMINT capabilities and those of the military services have been much greater. The ASD/C3I is in a position to see these problems but virtually is without the means to solve them.

CI programs are trivial in size compared to all other intelligence programs, but their coordination within OSD has no truly effective mechanism. Thus they are another resource management problem reflecting the absence of line program management authority above the military services.

Within the GDIP, things are not much better. Although GDIP is a consolidation of programs under the director of DIA, he cannot effectively judge input-output relations in a PPBS manner because they include

such a diverse and often disconnected set of activities. Many of them are intelligence analysis, but they also include HUMINT collection and some technical collection. The director of DIA is not at all in a position to judge the overall utility of his IMINT and SIGINT (ELINT) programs. Nor is he in the best position to judge the HUMINT programs, although here he has a better perspective on expenditures and the collection results. He is best positioned to judge intelligence analysis programs, especially for support to materiel and force development, but also for support to military operations and planning.

To sum up, the system for resource management of defense intelligence leaves a great deal to be desired. That has long been clear from the complaints by both the Congressional intelligence committees and the Armed Services and National Security committees. Apples and oranges are mixed within the various programs. Fragmentation also characterizes several areas. Program management structures are missing in a couple of places. Overall, a rather chaotic picture emerges, not unlike the picture of support to current operations and materiel and force development as described above. In some respects, the fragmentation in one is a reflection of fragmentation in the other, and vice-versa. Managers directly responsible for intelligence “outputs” do not have adequate responsibility for “inputs” on the resource management side.

Can Structural Changes Improve Defense Intelligence?

It can be argued that the system seems to work – more or less. But does that mean nothing can be done to make major improvements? One might insist that improvements are largely a matter of better management and leadership, but that is really not convincing. The major problems, as the foregoing review has tried to show, arise in large part from the structural arrangements. They are not at all consistent with the principles set forth in the section on doctrine for intelligence operations or for resource management. That is why significant improvement confronts obstacles beyond the power of managers to overcome.

The first glaring violation of those principles is the potpourri of activities—analysis, collection, and so forth—lumped into DIA. The fragmentation of CI is another. Even the intelligence analysis function, clearly the core of DIA, is organized in less than a coherent fashion. No clear organizational distinction between intelligence support to current operations and support to materiel and force development is drawn. And, in light of the principle of unifying each intelligence collection discipline, there is no justification for DIA to be in the collection business at all. What it really needs to emphasize is its collection management capabilities for maintaining access to the national collection systems for SIGINT, IMINT, HUMINT, and CI. Competing with those systems (where they now exist) is not a productive endeavor.

Clearly, major structural changes could be made that could bring improvements in performance, both in intelligence activities and resource management. The present organizational arrangements and program responsibilities ensure that significant improvements are not possible. Figure 4 illustrates the recommendations below, as they pertain to the Defense Intelligence Agency.

Recommendations

- Implement all the recommendations for the DCI's management structures and those for SIGINT, HUMINT, IMINT, and CI. These reforms impinge directly on the DoD intelligence structure.

To deal with reform in DoD intelligence, we must assume that recommendations made for the DCI's IC management mechanisms have been implemented. To implement the changes in IMINT and HUMINT, and to give the national manager for SIGINT full authority over SIGINT, would require transferring DIA's collection activities. Both its technical collection (SIGINT and IMINT) and its HUMINT, clandestine and overt, would be turned over to the national managers of these collection disciplines.

- Keep the Defense HUMINT Service as a single DoD organization under the OPCON of the CIA/DO.

This change makes the director of the CIA/DO effectively the "national HUMINT manager" within the IC. At the same time, it does not solve a nettlesome problem for wartime clandestine HUMINT support to military commanders because the CIA/DO is not under the directive authority of the Secretary of Defense as NSA and NIMA are. Can the Secretary of Defense, therefore, be sure that the CIA/DO will be responsive to taskings from unified commanders? This is not an academic issue; it has troubled almost every military operation since 1947. Support to military operations has always been extremely low among the CIA's internal priorities, leaving it ill-prepared to respond to military requirements. If the DCI is willing to make the CIA/DO responsive, it will be, but if not, only the President can overrule him. Presidents have a poor record of settling such disputes. The obvious organizational answer is to subordinate the DO to the Defense Department, like NSA, NIMA, and DIA. But the DO's relations with State, its CA responsibilities, and several other factors would be complicated by that change. The study, therefore, recommends no specific solution but rather flags it as a continuing problem for the President, the Secretary of Defense, and the DCI.

- Create an overt HUMINT organization within DoD as a joint activity that coordinates its activities with the national HUMINT manager (CIA/DO).

This organization should manage the defense attaché system as well as all of the debriefing programs, including OPCON over some of the military service debriefing and interrogations capabilities when they are not committed directly to unified commands. The model for this organization should be a news service such as Reuters or AP. It needs a communication system that allows military attachés, interrogators, debriefers, and other reporting assets to be managed as a network of journalists is directed by a central editorial and production unit. These activities, of course, should not only be coordinated with the national HUMINT manager in connection with his responsibilities for a national overt HUMINT collection system. They should, in many cases, be under his OPCON as well. Only then will the national HUMINT manager be in a position to deal with his overall resource management role for overt HUMINT.

- Put all DIA's ELINT collection under NSA. Put its IMINT collection under NIMA.

If intelligence analysis units in the JCS or DIA need ELINT, they should task NSA to provide it. For IMINT, they should task NIMA. For MASINT and other special collection, the DCI should assign the collection responsibility to one or more of the collection disciplines. NSA and NIMA can do some of it. The DO will

also have to deal with some of these requirements. MASINT and related new technical collection requirements have been a management problem for some time, and need the DCI's constant attention as the technologies involved emerge and proliferate.

- Create a DoD CI management center with OPCON, policy, and program management authority over the military service CI capabilities.

This organization should take charge of DoD CI above the tactical level, and it should relate DoD CI to the national CI management system.

- Abolish the NRO and transfer its program offices to NSA and NIMA.

This change is explained in detail in the sections on DCI management structures, and the SIGINT and IMINT collection disciplines. It needs no further comment here except to point out the implications for DoD intelligence program management. Major collection agencies should not have large portions of their operating assets funded through an independent DoD program. SIGINT, IMINT, and most HUMINT program management will fall under the national managers of these collection disciplines. These national managers will deal directly with the DCI in his management of the NFIP, not through an intermediate line management authority for all DoD intelligence programs.

All of the foregoing changes are essential to make DoD intelligence structure fit the reforms of the IC at large. What additional structural changes make sense within DoD?

- Using DIA spaces, create a formal J-2 intelligence organization on the Joint Staff for SMO, essentially a J-2 analytic support agency.

This organization would be committed almost entirely to current intelligence. It must have communications links with all J2s in the unified and specified commands, and it must collaborate with them to meet operations and planning needs. It should also manage the program budget for its own and all the J2s. Without this resource control, it will never be able to construct adequate communications, ensure a common doctrine for operations, or ensure that all the J-2s are properly staffed and equipped.

All of the personnel and resources for this organization would come from those elements DIA has traditionally devoted to its JCS support element. This office would be headed by a two-star military officer.

- Make the Director of DIA the coordinating manager of all intelligence support to materiel and force development—both joint and by the services.

While this organization must perform selected analysis, both general military and S&T, and while it must keep adequate data bases for research and analysis support, it should allocate, as it now does, the bulk of the analysis to the military services. It must be active in overseeing and encouraging the service analysis efforts, not competing with them. This organization can also be extremely helpful to the DCI if it works with the NIC and its DI in sorting out the more effective divisions of analysis responsibility within DoD and the military services.

- Create a red-blue net assessment center within DIA responsible directly to the Secretary of Defense.

Net assessment has traditionally been a point of contention between CIA and DoD. The Joint Chiefs and the Secretary of Defense have rightly argued that because they have final responsibility for judging the required size and types of military forces needed to defend the country, they must also have full authority over net assessments. If such assessments were done by CIA, and if they unjustly overvalued blue forces or undervalued red forces, political groups in Congress and elsewhere would use these assessments to oppose an adequate U.S. military force structure.

Notwithstanding the validity of this argument, the Joint Chiefs and the Secretary of Defense have never really found a way to do joint net assessments themselves. Each service fears that it could lose force structure or programs as result of such analysis. Thus the Joint Chiefs agree to disagree by refusing to accede a joint net assessment capability which they cannot fully control.

If the military services cannot agree among themselves, there is nothing to prevent the Secretary of Defense from creating his own personal net assessment capability. Using DIA resources for its creation within the DoD intelligence structure would be a very effective approach. The "red" data would be fully available to it. And OSD/PA&E (Program Analysis and Evaluation) could make available adequate "blue" data. The service chiefs might quarrel with the Secretary about this organization's analysis, but they could hardly object to his directing that it be done. Moreover, it would be accomplished by DoD intelligence personnel supplemented by people with special skills and training in net assessment techniques and military officers with knowledge of military operations.

There is now, of course, an OSD Office of Net Assessments. Its unique leader, Mr. Andrew Marshall, has made it an effective advisory office to the Secretary of Defense, but it has never been allowed to perform the kind of joint force assessments that would yield highly useful information for making program decisions about force structure and weapons systems.

What the Secretary would do with this analysis by a new net assessment center is another issue, but in principle he could use it to strengthen his arguments for various weapons systems and force structure mixes. It could be as powerful a tool for him as PPBS was for McNamara, only it would seem to have greater and more varied possibilities because net assessments require deep expert knowledge about actual military operations, not just micro-economic analysis and operations research and systems analysis (ORSA) skills focused primarily on "inputs" of resources. Net assessment begins with the "output" end of the analysis, and for that reason, it could be superior to PPBS as it was practiced under Secretary McNamara.

Conclusion

This review of the present state of DoD intelligence has identified a sufficient number of structural problems to make a compelling case for structural reform. Much of it is necessary to accommodate reforms in the collection disciplines and the DCI's IC management structure. Other parts of it are demanded by dysfunctional aspects of the present organization.

The recommendations offered as remedies are imperative where they are necessary to accommodate reforms of the larger IC. The other recommendations are primarily suggestive of how the doctrinal principles, set forth in an earlier section of this study, may be applied. Variants of them might prove to be better solutions, and a few of them might prove difficult to work effectively. The main point remains, however, to point the way for reform by offering fairly specific recommendations for structural changes. Closer analysis of some of the realities and problems will undoubtedly require that they be modified, even dropped in some aspects, or quite different approaches taken. Getting going and going in the right directions are the truly important points to conclude from both this review and its recommendations.

Notes

1. One DoD organization, the Defense Airborne Reconnaissance Office (DARO), is not treated in this study. It is a relatively new organization intended to overcome the fragmentation in the development of aerial reconnaissance platforms among the military services and the IC. In principle it is likely to create some of the same problems generated by the NRO, but that remains to be seen. Because no obviously more effective alternative structure is easy to conceive for this troublesome area of R&D and resource management, it was decided not to examine it in this analysis.

2. In addition to the NFIP and TIARA, the Joint Military Intelligence Program was established in 1994; most of its programs were previously in TIARA. The JMIP funds programs occupying a middle ground between national and tactical. Defense-wide, multi-service, joint activities are to be funded under JMIP. Programming for the JMIP is the responsibility of the Assistant Secretary of Defense for C3I, the Directors of DIA, NIMA, NSA, the Director of DARO, and the Defense Support Project Office. Dan Elkins, *An Intelligence Resource Manager's Guide*, 1994 Edition (Washington: Defense Intelligence Agency, Joint Military Intelligence Training Center, 1994), pp. 100-101. The editor of this study wishes to express his thanks to Mr. Elkins for reading one of the drafts and making many helpful comments.

3. Elkins, p. 38.

4. Elkins, pp. 41, 42.

5. DoD, Directive 5205.9, April 7, 1995 (mimeo fax).

6. Dan Elkins, "Updates to 1994 Edition of An Intelligence Resource Manager's Guide," November 1996 (mimeo fax), p. 3.

Section V

The Signals Intelligence Discipline: Structure and Management

Introduction

Of all the intelligence collection disciplines in the IC, SIGINT is the best structured to exploit changing technology and to provide support both to national-level users and to tactical military forces. This is true primarily for two reasons. First, in the early 1950s, the military service SIGINT organizations were centralized under a new organization, the National Security Agency (NSA). The military services' SIGINT organizations, Army Security Agency (ASA) and the Naval Security Group (NSG) in particular, strongly resisted the change, and they were able to prevent NSA from gaining program budget control over their tactical assets. They also maintained independent SIGINT commands, so-called "service cryptologic elements" (SCEs), but their program budgets were put under NSA management, and their collection assets above the tactical level were placed directly under NSA's operational control.

At the same time, however, NSA's independent budget authority and its autonomous personnel system for recruiting civilians with appropriate technical and other skills created a concentration of resources devoted entirely to signals intelligence under a single director. This allowed a rapid evolution of technology in NSA's R&D programs, permitting NSA to field systems rather rapidly. The nature of its work, concern with communications, gave NSA a strong impetus to build its own large and flexible communications system. As space communications were added to ground communications, NSA rapidly built a global communications system to handle its collection activities. The result has been a fairly dynamic process, causing constant adaptation in the SIGINT system over the postwar decades.

Thus NSA comes close to providing a "national manager" system for SIGINT because of its early unification and the nature of its business, technology and communications. Among the intelligence collection disciplines, therefore, it is in the best shape and least in need of major structural change. Still, it has internal problems. It also has one large structural problem that must be overcome before its director can perform an effective role as the national SIGINT manager.

What follows is a general description of the SIGINT system and some of its problems. Thereafter, its structural problem, lack of full control over the national SIGINT program, will be examined. Finally, recommendations for changes will be made.

The SIGINT System

The core of the SIGINT system is NSA. It is best understood as a “unified command” within the Department of Defense and also as a “military service.” In other words, NSA is really a microcosm of the Department of Defense itself.

While the most demanding cryptanalytic work, supporting R&D, and procurement are performed by NSA’s work force, NSA also depends heavily on military personnel for most of its collection activities. The military SCEs (Army’s Intelligence and Security Command [INSCOM], the Naval Security Group [NSG], and the Air Force Intelligence Agency [AIA]) operate NSA’s many field collection sites as well as mobile collection systems. Command of these sites and activities remain with the SCEs, but operational control belongs to NSA. This distinction, of course, comes from the doctrine for unified military commands. A unified command normally has an Army, Navy, and Air Force component command. These commands handle discipline, logistics, personnel, finance, housing, pay, medical services, and all of the traditional command maintenance responsibilities. For the conduct of military operations, however, the joint commander and his staff enjoy operational control. In other words, they give the orders and direction for combat operations. The Army, Navy, and Air Force component commanders do not. If this doctrinal concept of joint military operations is understood and applied to NSA’s relation to the SCEs, then the system of operations is clear. Actual collection and processing of signals is an OPCON matter. The authority for SIGINT operations remains with the director of NSA. In fact, he is the “joint” commander as is any CINC of a unified command.

This approach to SIGINT operations has allowed a highly effective system to emerge in which most of the field operations are handled by the SCEs while the more complex tasks of organizing and controlling the system are left to NSA. Relations between NSA and the SCEs, however, have not been trouble-free. At times, the military services have pulled tactical SIGINT capabilities away from NSA’s OPCON. Serious disputes have always surrounded these moves, and they usually thrive on the lack of a proper technical understanding of the SIGINT system and process by the military services. NSA’s organic components have also contributed to the disputes, not least because many of its civilian specialists are not very familiar with the SIGINT needs of military combat operations.

A number of crises, such as the Iran rescue attempt in 1980, the Libyan raid in 1986, and the 1991 Persian Gulf War, helped push aside some of these turf disputes in favor of effective innovations in tactical SIGINT support. Some commanders in the military services have come to understand that having their tactical SIGINT assets coordinated within the overall system is a huge advantage. And NSA has used its vast communications system to ensure rapid and effective dissemination to tactical forces of SIGINT products collected by national systems. In other words, through effective central OPCON, NSA has been able to bring to bear the entirety of the SIGINT system—space-based collectors, collection sites far from the zone of military operations, and cryptanalytic and linguistic skills that the military services cannot afford or maintain—for support to tactical operations.

Progress toward an effective use of the entire system for tactical support, however, is not a simple matter. It requires rapid innovation in each case, and it also requires a mix of technical skills brought to bear in a

cooperative fashion to work out effective OPCON plans and directives. Civilian personnel with deep technical knowledge must cooperate with military personnel with equally deep knowledge of military operations. Tensions are inevitable, but because NSA's Director is a military officer in the DoD chain of command, progress has been possible. Like any other CINC in the joint system, the director of NSA has to respond to his commander, the Secretary of Defense, through the Chairman and the Joint Chiefs.

Viewing NSA as a "unified command" provides an important but incomplete understanding. NSA is also analogous to a "military service." It recruits and trains its own personnel—the civilian component of the SIGINT system. It has its own R&D and procurement system as well as its own logistics system. In these regards, NSA is very much like each of the military services, though much smaller. As in the case of its operational connections to tactical military units, NSA has traditionally had turf struggles with the military services in R&D and procurement of tactical SIGINT systems. Within the Defense Department, these programs are controlled by the services and included in the Tactical Intelligence and Related Activities aggregation, with the joint portion of such funding found in the Defense Cryptologic Program (DCP).

Drawing a clear line between NSA and military services in this complex program area is difficult. Not only is it difficult to designate some elements of these programs as purely SIGINT because they are mixed into non-intelligence program elements, but it is also impossible to declare all the personnel involved in their operations as belonging only to intelligence duties. These turf problems, therefore, will likely remain unresolved, to be accommodated and managed, not eliminated.

In one regard, however, the military services and their SCEs could improve the situation. That concerns R&D for tactical systems. By insisting on independent R&D for tactical systems, the services deny themselves the vast advantages of R&D management experience that NSA possesses. Occasionally a military service has simply taken NSA-developed systems and adapted them for tactical use, and to great advantage, both in cost and in the time required to field them. Progress has been made on this front, and it should be encouraged. The military services already face such diverse R&D challenges that they cannot possibly compete effectively with NSA's more narrow focus on SIGINT systems.

A number of other areas, outside the Department of Defense, involve both operational and R&D turf issues between NSA and other IC components. For reasons of security, they cannot be discussed, but they are manageable, not major systemic problems.

(NSA also has responsibility for a large non-intelligence function. It manages and develops the national cryptologic system, that is, all cipher devices and codes. It performs this service not only for the Defense Department but also for all federal agencies which need secure communications. This function, of course, lies outside the bounds of this study.)

Thus far, this review of the SIGINT system has dealt only with its support of military operations and its resource issues with the military. NSA also provides SIGINT support to the White House, State, CIA, and many other users. The system for this support has generally worked very effectively. Thus it does not need major reform attention. Certain aspects of it, however, are instructive to note when considering IC structural reform.

NSA is a combat support agency within the Department of Defense. At the same time, a large number of its customers are outside of military circles in purely civilian agencies. And the customers have been generally satisfied with the support they receive. The significance of this record is very important. It means that “military intelligence” organizations can provide abundant and satisfactory intelligence support to non-military users.

On occasion, members of the Congressional oversight committees make an issue of whether or not an intelligence agency is within or outside the military because they assume that those agencies within the Department of Defense will neglect civilian intelligence needs. NSA’s record is compelling evidence for rejecting that assumption.

It is true that within the military services concern has been raised about their resources in the SCEs being used to produce intelligence for non-military users. Highly ill-advised policies about the use of their tactical SIGINT personnel have sometimes been imposed. Still, these sentiments and resulting actions have never had a noticeable impact on NSA’s support to civilian users. And in some cases, these military policies have been reversed when it is realized that keeping military personnel outside the active SIGINT system prevents them from maintaining adequate skills for actual military operational support.

The reverse concern, that civilian intelligence collectors will not provide effective support to the military services, is genuine. In the HUMINT and CI areas this has always been a notorious problem, and the same is true, although for different reasons, in IMINT.

Space-Based Collection Systems

The National Reconnaissance Office has the responsibility for procuring and fielding space-based SIGINT collection systems. Several decades ago, when such systems were new and very few, NRO was highly effective in pushing the frontiers for SIGINT collection from space. The NRO, however, was and remains largely an R&D and procurement organization, not an intelligence organization. It consists almost entirely of contracting officers and technicians overseeing private-sector vendors who make the systems. NRO is thus analogous to the R&D and procurement commands within the military services. This is a very important point to keep in mind for understanding recommendations this study will make concerning the NRO. The NRO has its own budget which it defends in the Congress and executes independently. No other purely procurement agency in either the IC or the military services has this autonomy. All others must let their budgets be integrated within a single military service’s budget or within an intelligence agency’s budget.

To clarify this point more sharply, suppose that the Navy systems command had a budget beyond the control of the Chief of Naval Operations and his staff. Suppose the systems command had almost complete control over what it chose to do for R&D, what it preferred to procure, and how much it chose to spend. Suppose what is spent was taken from the Navy’s own budget. The only connection to Navy it would acknowledge was to accept “technical requirements” for defining the performance of the ships and aircraft it developed and purchased. That is, the Navy would be allowed to specify the size and speed of combatant

ships, the range and weapons performance for aircraft, and the like. The systems command, however, would retain the discretion to procure bigger or smaller submarines, surface ships, and aircraft carriers. It might prefer to build many aircraft carriers and very few submarines, or vice-versa. It might prefer to build only cruisers, neglecting destroyers and mine-sweepers.

If the systems command had this discretion, organizational theory would predict that systems command would tend to choose to build those things that caused its budget to be as large as possible. Actual naval operational requirements for combat missions would be secondary. The vendors with which it does business would lobby Congress strongly to defend the systems command's autonomy because they would become partners with it in dreaming up more expensive and technically exciting projects. And to the degree this drive for an increasing budget succeeded, the Navy's budget for all other activities would have to absorb reductions to meet the growth of the systems command.

Now, let us return to the SIGINT system and the NRO. Over time, constellations of collection systems emerged, and as NSA learned more about how to use them, not only together but also in conjunction with earth-based systems, the approach for the SIGINT exploitation of space systems gradually changed. Increasingly, NSA became capable of looking at mixes of space-based and ground-based collection systems working synergistically. Cases arose where a far better overall SIGINT capability could be obtained by cutting back space programs proposed by the NRO and using the funds for non-space systems or for additional numbers of space systems that the NRO preferred not to procure. Disputes arose over the mix of various space-based systems themselves. From its operational viewpoint, NSA preferred one mix, the NRO another. The reasons for the NRO's preference are not hard to discover if one recalls the foregoing example of the Navy's systems command controlling its own budget separate from the CNO and his staff. The systems command logically would seek the more expensive programs, not those that necessarily fit the CNO's needs for an overall naval capability. That is precisely what has increasingly occurred in the relations between NSA and the NRO. The resulting turf battles and budget quarrels reach the Congressional oversight committees. The committees are naturally perplexed by them, but they have never fully understood why they occur. The issue is not a matter of personal relations between NRO and NSA managers. It derives from the very structure of the resource flows, the incentives they create, and the demands by SIGINT users for better support. Both agencies could be staffed with "saints" who agreed to forget all the turf issues, and in the course of one program cycle, all of them would reappear.

The NRO not only competes with NSA for funds within the National Foreign Intelligence Program; it has expanded beyond that area. In its so-called TENCAP (Tactical Exploitation of National Capabilities) program, NRO has solicited funds directly from the military services by promising them direct down-link intelligence from space systems. As experienced SIGINT personnel could easily point out, most SIGINT collection requires large amounts of human involvement in processing, and SIGINT collected from space seldom is usable without other kinds of SIGINT added or taken into account. Thus the very idea of independent TENCAP was based on an incorrect premise. Yet years of spending on TENCAP passed before the military services began to realize that they were not getting much for their money. TENCAP was simply a mechanism for obtaining funds for the NRO from TIARA, in addition to its usual source of funding, the NFIP. NRO personnel have little or no comprehensive understanding of what is involved in providing usable tactical intelligence. Thus they can honestly push technical schemes that on the surface appear

feasible but in reality are not [1]. Limited technical understanding within the military services on such matters qualified them as easy targets for these schemes.

If the NRO's portion of the national SIGINT budget were a trivial amount, the problem might be written off as an acceptable bureaucratic overhead cost. But it is not. During the 1980s, it averaged about 40% of the SIGINT budget. The director of NSA cannot, therefore, answer effectively to the DCI in advising him on the national SIGINT program. Nearly half of it is kept entirely hidden from him by the NRO.

Because of the amount of money spent on overhead collection systems, this structural problem in the IC probably accounts for vastly more wastage of financial resources than any other. The potential savings have at times been huge—in one case, \$6 billion over a Five Year Program.

Recommendations

1. Make the director of NSA the national manager for the SIGINT program and for operational control and management of the entire system.

The most important change required to make the director of NSA the national SIGINT manager is the elimination of the NRO and its independent budgetary authority, allowing the national SIGINT manager to make the R&D and acquisition decisions in his discipline. NRO's working components, however, must be retained. They have invaluable expertise and long experience in contracting with the aerospace industry for developing and fielding space systems. They could not be easily replaced. They need fundamental realignments in their programs, however, as well as a different fiscal management authority to replace the NRO headquarters. That can be done as follows:

- Place NRO's SIGINT space systems development and procurement program offices under NSA.
- Assign all space imaging systems development and procurement to another program office, for IMINT. (Control of its program budget should fall under the new National Imagery and Mapping Agency, as explained in the study section on IMINT.)
- Include the budgets for the SIGINT development and procurement program office(s) within NSA's Consolidated Cryptologic Program.

The consequences of implementing these recommendations should be apparent. The NRO program offices would remain with a specialized allocation of programs, not a mix of SIGINT and IMINT programs as they traditionally have managed. They would no longer depend on the NRO to handle their program budgets and to present them to the Congressional oversight committees. Instead, SIGINT program offices would look to NSA for that function. The IMINT program office would look to NIMA for that function. Figure 6 illustrates the reassignment of NRO programs to NSA and NIMA, as well as the organization of national agencies for HUMINT and CI.

Four critically important advantages will accrue if these changes are implemented. First, the vicious turf fights between NRO program offices will disappear because they will no longer each be producing both

SIGINT and IMINT systems. The mix of both kinds of systems in each program office has engendered unhealthy competition. They conceal technology from each other. They fight for control of each new SIGINT and IMINT program. And these struggles make life difficult for the private sector vendors in dealing with both offices.

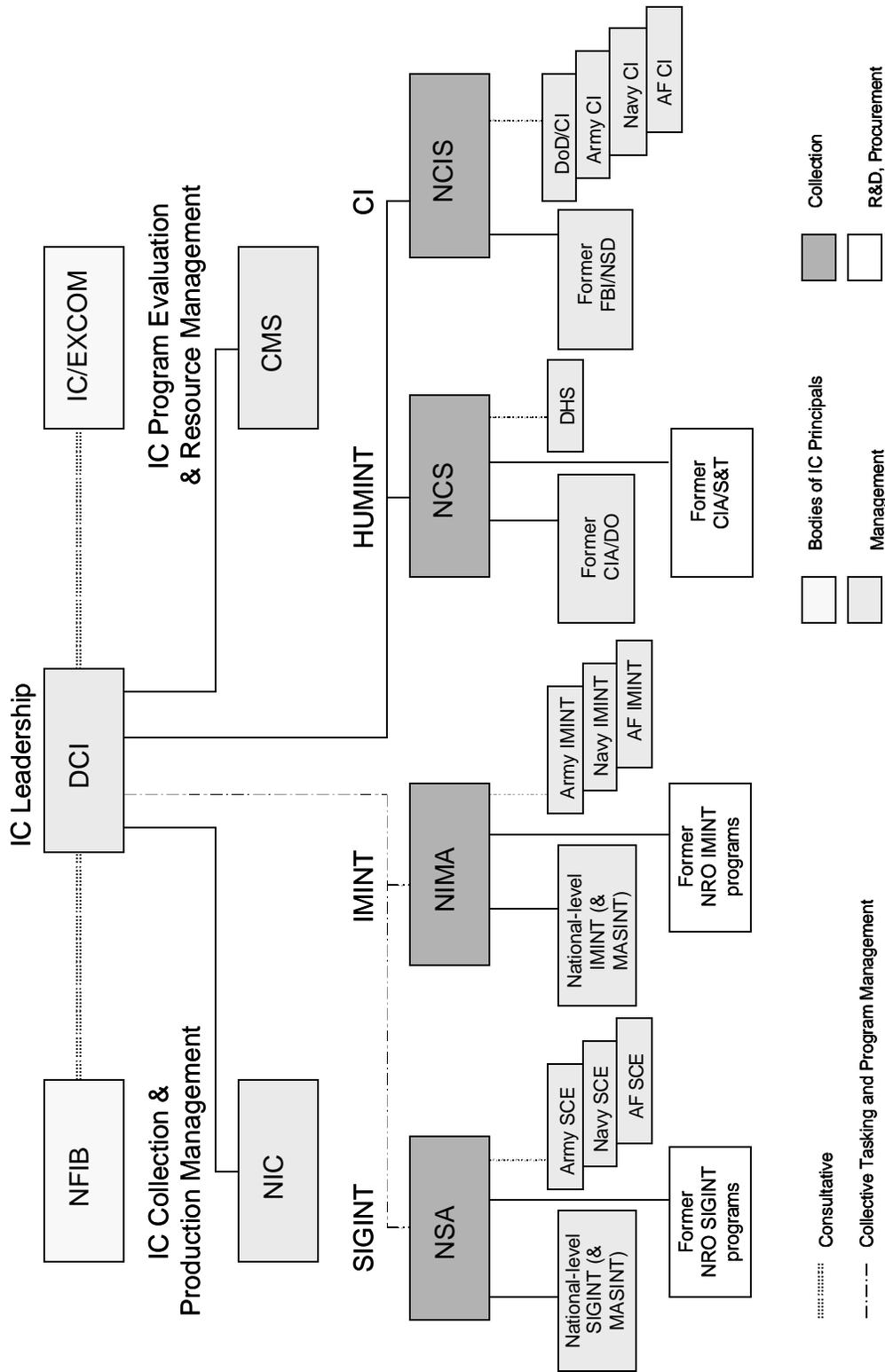


Figure 6. Management and Collection Elements of a Reformed U.S. Intelligence Community Arranged by Function

Second, space-based SIGINT systems will be traded off against other systems, ground, air, sea, and mobile. More effort to use space-based systems in conjunction with earth-based systems will be possible because the opportunities can be considered in the R&D phase, not left to chance after they are deployed. The autonomy of the NRO prevents that today. More innovation in using constellations of space systems in a coordinated manner is also likely.

Third, the endless turf fights between the NRO and NSA over management and targeting of space-based collectors should abate. A huge step in reducing this problem was accomplished in the early 1980s with the creation of the Combined Overhead Collection Management Center, but it merely papered over many of the problems. It did, however, give NSA the capability to re-direct overhead collection rapidly at any hour of the day or night. Previously permission to re-direct such collection was controlled by a committee under the CMS's predecessor, the Intelligence Community Staff. Since this committee was available only during weekday official business hours, it could not respond to crises on weekends and at night. Ridiculous delays were the product of NRO turf prerogatives. With the dissolution of the NRO, there would be no question about NSA's (and NIMA's) authority for re-targeting. And the artificial boundary at ground control stations between NRO "management" of the satellite and NSA's (and NIMA's) "processing" of its collection could be removed, bringing an end to yet another set of NSA-NRO turf fights and enhancing management efficiency within these stations.

Fourth, the TENCAP program would disappear. Progress in more and faster support to tactical forces would result because the military services would have to look to NSA for it instead of seeking to go around NSA through the NRO's TENCAP program. If NSA were not responsive, the Joint Chiefs could take up the issue with the director of NSA, and responsiveness would be forthcoming.

2. Direct the military services and NSA to make greater efforts to coordinate the CCP with the Defense Cryptologic Program in the Joint Military Intelligence Program, and with tactical SIGINT programs in TIARA.

This recommendation is little more than a platitude, but it bears frequent repeating. The Army has been weakest in taking advantage of collaboration with NSA in this regard, and the Air Force has not been exemplary. The Navy and the Marine Corps make the most use of it. A number of joint service programs for platforms that could carry SIGINT systems have not been as fully connected either to the DCP or the CCP as they might have been.

As a part of this recommendation, if the lesson has not yet been fully learned about the necessity of a "technical control" communications link with NSA to every tactical SIGINT unit in existence, then the Secretary of Defense should order the military services to ensure such links are established and permanently maintained.

3. Direct the DCI to use his CMS Science & Technology Office for an examination of several extremely sensitive and core capabilities in NSA.

Periodically in its history, NSA has been subjected to an outside investigation of technical experts and scientists to review the health of its strategies, technologies, and other sensitive issues in light of the state of modern communications. Precisely why this has been necessary is not possible to explain in an unclassified study. It may be that such a review is not now needed, but the communications revolution of the past decade and the continuing dramatic changes suggest that it be considered. It has to be a “friendly” review, not one with punitive overtones. And if properly conceived, it would likely be welcomed by NSA.

Conclusion

Clearly the most important recommendation for SIGINT is the first, concerning the dissolution of NRO and placement of the SIGINT portion of NRO's programs under NSA management. The second and third recommendations are not nearly as critical. Moreover, most NSA directors have been painfully aware of the issues related to these two recommendations, and they have struggled with them. Most everyone is aware of the problems involved in coordinating the CCP and DCP/TIARA, and no easy or sweeping solution is possible. Thus it remains a permanent management issue, not one amenable to IC structural reform.

The first recommendation—involving the dissolution of NRO—however, concerns a problem that no director of NSA alone can solve or even make marginal progress in ameliorating. It requires a major outside effort because it involves dramatic shifts of bureaucratic turf and budgetary responsibility. The amount of money that has long been wasted as the result of delaying a structural solution is large. Finally, only by implementing it can the DCI have a “national manager” for SIGINT as the recommendations for reform of his management structure require.

Without it, the DCI cannot hope to impose a PPBS approach on the NFIP. As long as he cannot, his IC management powers will remain severely limited. DCI's traditionally come to that post with little experience or understanding of the technicalities of the NRO-NSA issue, and they are confronted with arguments from within CIA that maintaining the NRO is absolutely essential to CIA's bureaucratic power and leverage over large funds spent primarily from the DoD budget. CIA's bureaucratic leverage, however, does not enhance the authority of the DCI over the IC. On the contrary, it helps prevent a genuine sense of “community” in the DCI's IC.

Note

1. NRO continues to mislead intelligence users and the Congress by marketing itself as an intelligence producer. See prepared testimony by NRO Director Keith Hall, before the Senate Armed Services Committee, March 12, 1997, p. 4.

Section VI

The Imagery Intelligence Discipline: Structure and Management

Introduction

Maps, drawings, photographs, and more recently, a variety of advanced technological means for acquiring and portraying images have only recently been grouped as a single intelligence collection discipline in the U.S. intelligence community. Although the acronym, IMINT, has come into common use, it has yet to acquire the status of a specialty on the same level as HUMINT and SIGINT. Even as the means for acquiring and transmitting images have involved highly sophisticated technology, requiring great technical skill and competence in its process, interpretation, and dissemination, IMINT has received neither a clear definition of its boundaries nor an organizational structure which permits full exploitation of contemporary IMINT capabilities.

This can be explained in part as the result of the natural fragmentation of IMINT in earlier times. Drawing was long a standard skill for army officers, especially reconnaissance officers. Sketching terrain, panorama views, fortifications, ports, and the like was one of several standard crafts for engineer officers. Cartography also fell into the engineer's domain.

As photography became available, it was used by reconnaissance officers in wartime, and by military attachés and clandestine agents in peacetime. With the appearance of the airplane in World War I, aerial photography emerged as a key intelligence collection technique. During and after World War II, the Army Air Corps and later the Air Force naturally took the lead in this area, but the Army and the Navy also maintained such capabilities as well.

With new means of imaging—infrared, electro-optics, television, and others—gaining a place in IC collection activities in more recent decades, IMINT has come to play a much more critical part in the IC's efforts. Specialized aerial reconnaissance aircraft (e.g., the U-2 and the SR-71) were designed for no other mission but intelligence collection. The truly dramatic breakthrough, of course, has been space-based IMINT capabilities. And more recently, unmanned aerial vehicles (UAVs) have begun to be used extensively to gather IMINT.

This fairly rapid expansion of both IMINT technologies and platforms to carry them for advantageous views of IMINT targets has created a complex and rich array of intelligence collection means. Creating a coherent and truly professional IMINT discipline, therefore, is long overdue. It should be among the major aims of intelligence reform in the 1990s.

The Absence of an IMINT System

To the extent an IMINT system has emerged, it was for years too fragmented to deserve the label, “system.” Within the Air Force, however, one could speak of a limited system. Aerial photography became critical intelligence for targeting bombers. That caused the Air Force to put a large effort into aerial reconnaissance means. For peacetime aerial photography, however, Air Force means were not adequate to cover the Soviet Union’s vast territories in search of missile and other military capabilities. The CIA, using the NRO as its development arm, built the U-2 precisely for the Soviet target, and soon after, it succeeded in fielding IMINT capabilities on platforms in space.

These two centers—the Air Force IMINT programs and the CIA’s MINT programs—developed along separate lines. The Air Force was more concerned with wartime tactical IMINT support. The CIA focused on peacetime acquisition of the Soviet military “order of battle,” especially its ICBM inventory. An overlap between the Air Force and the CIA’s IMINT interests developed in the Strategic Air Command (SAC). Given SAC’s mission of being able to deliver large nuclear strikes on the Soviet Union, it needed the IMINT products that CIA was acquiring, but it also needed coverage of more than the military targets of interest to CIA analysts. New and growing space-based IMINT capabilities, fielded and largely controlled by the NRO, were able to meet both user demands.

The Navy and the Army also began to find uses for this new space-based IMINT production. They joined the queue of customers demanding priority for their targets. In the earlier period, IMINT technology for space required a considerable delay from the time of the imaging to the time it could be exploited by imagery interpreters. In other words, time-sensitive targeting was not possible with space-based IMINT; nor was it very rapid for Air Force tactical IMINT. Photographs had to be taken, returned for development, and then interpreted. These processes could take from weeks to a day or so, depending on the IMINT means.

Because the new IMINT technology was not initially able to respond to taskings with great speed, the system for its management was constructed with little or no consideration to rapid-response IMINT. The National Photographic Interpretation Center (NPIC) was established by CIA to meet the taskings. The Defense Intelligence Agency and the military services contributed personnel for imagery interpretation to the NPIC, but it remained within the CIA’s chain of command. To formalize and manage IC-wide access to tasking the space-based IMINT capabilities, the IC Staff created a committee, COMIREX (Committee for Imagery Exploitation), with representatives from all IC components. COMIREX managed the prioritization of IMINT tasking for all national IMINT systems. Military and civilian users alike queued up to place their requests for imagery.

In principle this made sense as long as IMINT products required several weeks to create. Speed was not a major issue except for support to tactical forces. These advanced national systems were not providing such support. They were supplying IMINT products to the military services, DIA, CIA, SAC, and a few civilian departments. None of these users were driven by “time sensitive” requirements. The unified commands in Europe and Korea, however, were another matter. They wanted IMINT that could “look” into the enemy’s rear and immediately provide target locations for air and artillery strikes, and they wanted equally rapid post-strike assessments. As new weapons systems with increasingly greater ranges began to appear, the

need for precise targeting data rose sharply. Cruise missiles and short-range ballistic missiles are examples. Attack helicopter units also needed better IMINT to facilitate their deployment deep into enemy territory. Even improved artillery was beginning to reach beyond the Army's organic target acquisition means. Only IMINT was able to provide target identification with sufficient accuracy to support these weapons systems. SIGINT could not pinpoint most targets, and HUMINT was too uncertain and most often non-existent.

Several developments occurred during the late 1970s and throughout the 1980s that account for the contemporary crisis in IMINT. First, advances in technology made it possible to produce near-real time imaging. The NRO—an R&D and procurement agency—was managing the operations of space-based imagery collection with these new capabilities. The NPIC remained the primary place where this imagery was analyzed. Next, the military services, especially the Army and the Air Force, were pressing ahead with a radar-imaging capability based on an aircraft: the JSTARS (Joint Surveillance Target Attack Radar System). SR-71s and U-2s were still carrying IMINT capabilities. And the older Air Force systems, such as RF-4s, and Army SLAR aircraft were still active. On the ground, electro-optic systems were being tried in experiments for support to ground force operations. Unmanned Aerial Vehicles with imaging capabilities were in development. Finally, a revolution occurred in cartography so that map-making was increasingly based on electro-optic imaging from space-based systems.

Another related development had a potentially revolutionary impact. As imagery was produced in digital form, it could be transmitted by wide-band communications anywhere in the world where adequate communications capacity existed. This meant that IMINT raw products could be transmitted directly to military units deployed for operations. Before this was recognized as a real possibility, IMINT products were derived by imagery interpreters in verbal form. These IMINT reports were transmitted as alpha-numeric text to users without accompanying photos where speed was desired. As long as this kind of product was acceptable, the NPIC and other centrally located IMINT production centers could send their products to tactical forces deployed anywhere. In practice, however, military commanders wanted their own organic intelligence analysts to have the photos.

The consequence of all these developments was the creation of a high degree of frustration among military users of IMINT. Technological developments had progressed rapidly, but the institutional developments that would allow these new IMINT capabilities to be used effectively for military operations were non-existent. Moreover, there was no organization that could be specifically blamed for this failure. Few if any military commanders, or their intelligence staff officers, knew how the IC Staff committee, COMIREX, operated. Some of them looked to the NRO's TENCAP program to provide the solution. Of course it could not. It did not have the communications or the personnel to manage the entire IMINT collection and production process. Its management did not even understand what that would involve.

The organizational vacuum for national-level IMINT capabilities is only part of the problem. A complete inventory of all the means of acquiring images of all types that now exist in the military services and throughout the IC would prove large and diverse, ranging from hand-held 35mm cameras to satellites with advanced digital imaging technology. The organizational locations of all the capabilities are no less diverse. No concept of managing these capabilities as a system exists, and any effort to create one would face significant bureaucratic resistance.

Predictably, during the Persian Gulf War, IMINT was judged seriously inadequate. General Schwarzkopf testified to the Congress on this point, expressing some dissatisfaction with his generally good intelligence support. Although he did not specify IMINT as the key problem, that was probably the primary basis for his remark [1].

The lack of an organization staffed with sufficient skills—technical and military operational—to take on the task of putting together a national IMINT system has been a major failing of the IC. The point has been made in testimony to the Congressional oversight committees several times. Senator Boren, in his draft legislation for IC reform in the late 1980s, recognized the problem and called for a national IMINT agency. Several other proposals of this appeared afterwards.

In 1993, the Defense Airborne Reconnaissance Office (DARO) was formed. DARO is a DoD organization charged with management oversight of the development and acquisition of all joint Military Department and Defense-wide airborne reconnaissance capabilities, including manned and unmanned aerial vehicles (UAVs), their sensors, data links, data relays, and ground stations. The hardware programs it manages are integral components of U.S. national IMINT collection capabilities. But DARO, like NRO, is an R&D and procurement office, not an intelligence office.

Only in October, 1996, was the National Imagery and Mapping Agency (NIMA) finally created. NIMA incorporates the NPIC, the Defense Mapping Agency, and the ground stations and mission control elements for all space-based IMINT systems.

This is long-overdue and welcome change, as far as it goes. NPIC naturally belongs to the core of a NIMA. Because IMINT provides most of the raw data for cartography, the Defense Mapping Agency (DMA) also belongs within the NIMA. When the idea of a NIMA was initially raised in the Defense Department, concern arose about mapping losing the priority it deserves. Having “Mapping” in the agency’s name should disallow neglect.

The logic of including the ground stations and mission control elements for space-based IMINT in NIMA should be self-evident. They are central parts of the present national IMINT capability.

Recommendations

- Designate the Director of NIMA as the “national manager” for IMINT. Ensure that NIMA’s structure allows the Director to exercise his responsibilities effectively, in particular, by carrying out the following recommendations:
- Place the NRO’s IMINT space systems development and procurement program offices under NIMA.

NRO personnel now run these IMINT programs. The general reason for this step is the same as for giving the director of NSA control of the SIGINT programs managed, as recommended in the SIGINT section. As national manager for IMINT, NIMA’s Director requires final responsibility for the budget now spent on NRO’s IMINT R&D, procurement and operations programs.

- Assign the primary coordinating and oversight role to NIMA for all military service IMINT programs.

- Direct NIMA to develop a system for exploiting all IMINT collection capabilities to support military operations (or any other operations) in a time-sensitive manner. This will, of course, require working out coordinated targeting and tasking arrangements with IMINT capabilities organic to tactical military units.

Precisely how to do this is beyond the detail into which this study delves. The concept, of course, is analogous to military SCEs under OPCON of NSA. The fragmentation of IMINT capabilities within the military services makes this a challenge, and many of those capabilities may prove best left as dedicated tactical assets under the direct control and tasking of local military commanders. In principle, those assets that have considerable deployment flexibility, such as U-2s and possibly JSTARS, should be placed under the OPCON of NIMA. Figure 6, in Section 5, illustrates the reformed NIMA along with the other national intelligence collection agencies.

Program management of IMINT will also remain somewhat divided between NIMA and the military services, just as SIGINT programs budgeted in TIARA belong to the services, rather than NSA. Many imaging systems are so organically tied to weapons systems and military units that their effective control is beyond what NIMA could effectively employ. NIMA, however, must be highly knowledgeable of all these systems in order to fit over them its array of IMINT capabilities, both those it owns and those under its direct OPCON.

Until a system for exploiting all IMINT collection capabilities is developed and practiced, the main advantages of NIMA will not be realized. The foundation for such a system is a world-wide communications structure. On the one hand this communications network must allow central control and direction of IMINT collection and processing. On the other hand, it must provide for rapid and effective dissemination of IMINT products to users. In some cases, those products may only be written reports based on the findings of imagery interpretation. In other cases, it will include direct dissemination of the imagery itself to users. Interpretation reports may accompany that imagery in some cases. In others, local imagery interpreters may process the imagery at the user level. Regional interpretation centers, located with unified commands, may prove the most effective solution.

There is no way to know in advance how best to structure such an operational system. Only trial and error combined with experience from actual military operations will allow NIMA to perfect such a system.

A key feature of this learning process will be working out methods which allow IMINT personnel with deep knowledge of the IMINT collection systems to design plans for rapid selection and tasking of the best available system to meet time-urgent IMINT requests. Knowing all available systems, the NIMA operations center should be in the best position to receive, prioritize (under JCS guidance), and respond to IMINT requests. It may choose an aerial IMINT platform, a space-based platform, or some other means to get the required imagery. And it must know how best to get the imagery processed into usable form and routed most directly to the user.

Although SIGINT operations are quite different from IMINT operations, there are parallels, and NIMA could take a number of lessons in this regard for handling crises and military operations where collection

assets must be rapidly redirected, communications quickly reorganized, and processing accomplished in an ad hoc fashion.

As NIMA works out its concepts of operations and designates tactical IMINT systems to be placed under NIMA OPCON, the Secretary of Defense and the Joint Chiefs will have to be strongly supportive. Bureaucratic turf issues will be serious, and if they are not addressed by the top levels of the Defense Department, they will place severe limits on the kinds of improvements in IMINT support that NIMA can provide.

Conclusion

Creating an effective NIMA will not be easy. Many bureaucratic interests will be threatened. Elements from several parts of the IC will be (and are being) forced to amalgamate in NIMA. They bring old ways of doing business with them. New elements, such as DMA, are joining the IC as well as NIMA. The process will require several years and even more adjustments when first efforts and schemes prove unworkable or ineffective. The potential gains from creating an effective NIMA, however, are simply too great to let the problems stand in the way.

The heart of an effective NIMA is to be found in two major features. The first is its communications system for managing both IMINT collection on a real-time basis and real-time distribution of IMINT to users. The second is its management of IMINT programs. If the Director of NIMA is given overall responsibility for IMINT, he will be in a position to make trade-offs among various systems, deciding the best mix of space, aerial, ground and other collection platforms and also deciding among the types of IMINT technologies—wet film, electro-optics, IR, radar imaging, etc. These two features of an effective NIMA would allow its director to have the kinds of information he needs to act competently as the DCI's national IMINT manager. And without a national IMINT manager, the DCI has little prospect for imposing a PPBS viewpoint on the IMINT portion of the NFIP. Recalling the section on a doctrine for the IC, it should be obvious that its principles are the guiding rationale for the recommendations made here for restructuring IMINT management within the IC.

Note

1. See U.S. Congress, Senate, Committee on Armed Services, Hearings, *Operation Desert Shield/Desert Storm* (Washington: GPO, 1991; S. Hrg. 102-326), pp. 320-321.

Section VII

The HUMINT Discipline: Review and Recommendations

Introduction

The heart of the HUMINT discipline is the clandestine service. A professional peacetime clandestine service is new in American history. Perhaps the most effective American clandestine operations were conducted by George Washington during the Revolutionary War, but after it was over, they were discontinued. During the Civil War the approach was mainly “privatization.” Pinkerton’s detective service ran clandestine operations on contract in support of Lincoln’s administration. Again, after the Civil War, clandestine HUMINT was discontinued. In the 1880s, both the War Department and the Navy Department initiated modest overt HUMINT collection by military attachés and officers on leave visiting foreign countries. Shortly before and during World War I, some clandestine operations were directed in Mexico because German intelligence was using Mexico as a base for its HUMINT operations. In the interwar period, military clandestine operations again largely ceased, although military attachés began more rigorous overt HUMINT activities. Still, they were modest in what they produced, and they were often naive in their judgments of both political and military affairs abroad. At the same time, the FBI under J. Edgar Hoover’s leadership began to engage in foreign clandestine operations on a modest scale.

Thus the United States entered World War II without an effective clandestine HUMINT capability. The story of Brigadier General William Donovan’s creation of the Office of Strategic Services is well enough known. By the end of the war it was extensive, especially in Europe, and it played a critical role in the late 1940s in undercutting Stalin’s covert operations aimed at communist party takeovers in France, Italy, and Germany.

It should be noted, however, that Donovan’s OSS was in many regards more heavily balanced toward covert action and paramilitary activities during the war than it was in purely clandestine HUMINT collection. As part of the War Department, the OSS moved into a vacuum. The Army’s intelligence capabilities were trivial at the time. After Donovan took over, he advanced HUMINT and covert action enormously, asserting a large degree of autonomy within the War Department. At the same time, the Army created the Counterintelligence Corps (CIC) which became reasonably effective, and it continued to play a key role in the occupation of Germany and the de-Nazification program.

Donovan always viewed himself as working for the President. He was able to recruit people into the OSS who would not have considered a career in Army intelligence after the war. The idea of leaving the OSS in the War Department after the war, therefore, was hardly acceptable to him. Moreover, the emergence of the Cold War in Europe made it clear that demobilization of the OSS would be a mistake. Thus in 1947, the OSS was made an independent organization, the Central Intelligence Agency.

Although the clandestine service was the core of CIA, Donovan and others made the case for a special CIA intelligence analysis element as well. They argued that the failure of Army and Navy intelligence to warn of

the attack on Pearl Harbor would again become a danger unless a national-level independent capability for analysis was created. These arguments prevailed, and the CIA's Directorate of Intelligence was added. The new DCI also created a National Board of Estimates to cap his warning analysis capability.

The Postwar Period

The Army did not wholly abandon clandestine HUMINT after the war. The Army's Counterintelligence Corps ran clandestine operations. The Air Force and the Navy also instituted rather modest clandestine HUMINT efforts. By the late 1970s, after a series of organizational changes in the military service intelligence organizations, the bulk of the Defense Department's clandestine HUMINT was in the Army. The Navy dropped out entirely, and the Air Force effort was extremely modest. The Army, however, had a fairly large and widely deployed HUMINT effort. All three military services retained active CI clandestine operations.

The CIA Directorate of Operations, of course, became the dominant part of U.S. clandestine HUMINT. Its relations with the Army's clandestine HUMINT varied from cooperative to competitive. Holding final approval authority over any military clandestine operation, the CIA/DO was effectively in control of the Army's capabilities and in a position to make them more or less effective.

In the first decade of the CIA's existence, its old close ties to the Army persisted. Army officers often served in the DO, and the Army's Special Forces, created for wartime covert action in the paramilitary area, sometimes worked under CIA control, such as during the Korean War and in Vietnam. As time passed, however, the relationship became strained. Among the more infamous CIA-Army affairs was Lieutenant General Arthur C. Trudeau's quarrel with DCI Allen Dulles over the degree of KGB penetration in the newly created West German intelligence organization, the BND. At the time, Trudeau was the G-2 of the Army, and his CIC in Germany had given him extensive and disturbing information on this point. Dulles flatly rejected it. During one of Chancellor Adenauer's visits to Washington, President Eisenhower invited Trudeau to make his case to Adenauer in Dulles's presence. Adenauer patiently listened to Trudeau and then asked who these KGB agents were. Trudeau unwisely handed him a list. Adenauer returned to Bonn and apparently took no action against them. The CIA and its creation, the BND, clearly won that round, but it left deep suspicions between Army HUMINT personnel and the DO at CIA.

For years, the quality of Army clandestine HUMINT was mixed. At times and in some places it was ineffective. The CIA worked assiduously to keep this impression alive and to make it appear to describe all Army HUMINT. Even the Army leadership became to share this judgment. In the early 1980s, the Chief of Staff of the Army initiated a study to determine whether or not to abolish Army clandestine HUMINT outright. The study was also to determine whether or not Army HUMINT, if it were retained, should be turned over to DIA and made a joint Defense Department organization. The study results were not fully acted upon, but a move to create a DIA clandestine effort began to take shape, and, in 1995, the Defense HUMINT Service (DHS) was formed. DHS consolidates military service HUMINT in one DoD-wide organization under DIA.

The quality of several Army HUMINT operations improved markedly in the early 1980s. Although the DO was never very cooperative in giving approval authority for them, a number of those that gained approval turned out to be successes. The Army made several attempts to work out a division of labor for clandestine operations, but they were never taken seriously by the DO. Part of the reason is to be found in the experiences of the Iran rescue attempt.

The Army needed intelligence on the embassy compound in Teheran, and it needed clandestine assets to provide assistance during the operation. The DO had no agents to provide this support and proved unable to develop them during the months of planning for the rescue attempt. The Army acted to fill the gap by creating the Intelligence Support Activity (ISA). This unit consisted of a mix of clandestine case officers and Special Forces personnel. A small number of them were able to pass as non-Americans and actually visit Teheran with some DO technical support. After the hostages were released, the Chief of Staff of the Army decided to retain ISA as a permanent organization to support any future operations of this type.

This did not please CIA. The saga of ISA's efforts to develop capabilities and the DO's obstruction of these efforts contributed to growing mistrust. By the late 1980s, a number of measures were taken to try to improve the climate. The most conspicuous was the assignment of a general officer to the DO. He was to be responsible for seeing that clandestine HUMINT assets for support to military operations were recruited and maintained by the DO. In reality, although DO-DHS relations have improved somewhat, this is not much of a solution. The military officer has no real power to insist on particular operational developments.

That the DO would not be very attentive to such developments is understandable. Its success, as it has always seen it, is not enhanced by maintaining networks of low-level assets. Rather it has always seen its mission as to penetrate the highest levels of political and military authority in target countries. The pressure to keep this focus was all the greater when the DO was periodically criticized by the Congressional committees and others for not having an abundance of this kind of HUMINT access. Neither the DO's self-image nor its ability to impress the President could be enhanced by the kinds of clandestine assets that are periodically needed to support military operations, e.g., in Iran in 1980 and in Iraq in 1990-1991.

Parallel to these troubled relations between the DO and military HUMINT, the DO maintained highly collaborative relations with Army, Navy, Marine, and Air Force special operations forces. In particular, Army Special Forces provided considerable resources and capabilities to the DO. In fact, the collaboration became so close that Army leadership supervision of it began to break down. The infamous "Yellow Fruit" episode, in which Army special operations personnel were operating outside Army regulations, arose in part because the DO had cultivated a sense of separateness and autonomy among the Army personnel with whom it had been working.

The Army's Special Forces have always been in search of missions, and many peacetime covert action programs have needed the very skills they possess. The DCI and CIA, of course, have full and unchallenged authority for conducting all such operations. The Special Forces can participate only at CIA's request. Most Secretaries of Defense, however, have been anything but enthusiastic about Special Forces' participation because of the record of covert operations becoming huge public relations problems, not to mention the connection of those operations to foreign policy disasters. Consequently, CIA has recruited and managed its own organic paramilitary capabilities.

To sum up the instructive conclusions to be drawn from this eclectic review of the DO's relations with DoD HUMINT, a couple of major points deserve emphasis. First, the DO in principle and authority is well-placed to be the "national manager" for HUMINT. The military clandestine HUMINT budget falls within the NFIP. And the director of the DO has final approval authority over any military clandestine operation. In other words, he has the same kind of OPCON over military HUMINT that the director of NSA has over military SIGINT operations. The DO could, therefore, take the view that military clandestine capabilities are part of the national HUMINT system and become deeply involved in their targeting and exploitation. That is the view that NSA takes of the military SCEs. The nature of clandestine operations, of course, is quite different from SIGINT or IMINT. Cooperation does not come naturally. Still, the director of the DO has all the authority he needs to take charge of military clandestine HUMINT. DHS resources devoted to clandestine HUMINT are relatively large. They could provide a dramatic enlargement of DO's overall capabilities. Moreover, the "quality" problem that has characterized the DO's disdain for DoD capabilities is not based on reality in many instances. And where it is, the DO has the power to help solve it: DHS case officers are trained in the DO's courses for clandestine trade craft. If the DO instructors give passing grades to military students who should not receive them, that is hardly the military's fault.

Second, two separate paramilitary organizations have grown up, one in the DO, the other in the Army's Special Forces and other DoD special operations forces. The military's strength is in military skills and operations. These are not the strength of the DO. Not surprisingly, DO paramilitary operations have generally been looked on by Army officers, when they have had the opportunity to review them, as amateurish at best, usually designed to fail. A close comparative look at the record of Army and DHS clandestine HUMINT operations and DO paramilitary operations would, in all likelihood, show that DoD has more justification for disdain for DO paramilitary capabilities than the DO has for DHS case officers. This raises the question of whether or not the DO should drop its paramilitary capabilities and depend largely on those in the Department of Defense.

Among the cabinet departments, the DO has its closest relations with State. Because of the general DO practice of maintaining "stations" in U.S. embassies abroad, the State-DO connection has always been intimate. Most of the time it has also been cooperative and mutually advantageous, but exceptional cases have made their way into the media at times, and very tense and counterproductive relations between the ambassador and the CIA Chief of Station (COS) are not all that rare. Do these troublesome cases indicate a genuine "systemic" or "structural" problem in the management and conduct of HUMINT operations?

The answer is "no," but with a caveat. The natural tendency for any COS and his case officers will be to limit the embassy's knowledge of its operations. Lives may be at stake, not to speak of operational results. A prying and skeptical ambassador can easily provoke the COS to leave him less than fully informed. Likewise, a COS can easily provoke deep distrust in the ambassador's mind by being less than forthcoming, causing the ambassador properly to pry into local HUMINT operations. When these operations involve covert action, the chance of State-CIA conflict increases dramatically. When clandestine operations only concern recruitment of spies, it is unlikely to escalate into a major problem. There is no organizational solution to this general problem. It is a management issue both for State and CIA. The problem can and has, however, taken on larger proportions when it links back to Washington and the DCI/CIA role in conducting foreign policy, and in those cases, covert action is almost always the root of the issue.

Most cases in which ambassadors and CIA station chiefs have been at odds to a degree that the matter has become public have their origins in differences between the Secretary of State and the DCI. The president has also been a key factor because he generally has encouraged or condoned the DCI's actions. If one looks closely at U.S. policy in Central America in the 1980s, this pattern is evident. It is also evident during the Kennedy administration in policy toward Vietnam although the dynamics were different. President Reagan was more clearly supportive of the DCI and his covert action programs in Central America, while President Kennedy appears to have lacked the leadership insights and experience to control ambitious subordinates, not just in CIA (e.g., Brigadier General Edward Lansdale) but also in Defense, State, and elsewhere [1].

Again, one is forced to conclude that solutions to these problems cannot be found in structural changes in the IC. They are policy problems, and they can easily be eliminated by rejecting covert operations as a policy instrument. With the end of the Cold War, inclination of presidents to resort to covert actions has already declined, but it will not entirely disappear. A number of challenges confronting U.S. policy in several regions of the world will continue to present the temptation. The point remains, however, that there is no salvation from these dilemmas in structural changes or shifts of responsibilities in the IC.

Finally, an old issue was raised in the 1980s concerning the DO's dependency on U.S. embassies as its primary bases of clandestine operations abroad. So-called "non-official cover" alternatives were encouraged as much needed additions. Again, this issue is not really an IC structural problem. It concerns clandestine operational techniques and does not belong to matters of IC management and structure. The expansion of the FBI abroad, specifically, the growing number of legal attachés ("legatts") overseas, is another issue that requires coordination and cooperation with DO. In the future, this development is likely to become a source of numerous problems.

A number of lesser but similar issues have been raised in other studies of IC reform. For example, should the DO be able to use positions in the media as cover for its agents? That is another "non-official cover" issue concerning clandestine techniques. It is serious issue, but this study will not address it. Nor will it address several other such issues concerning clandestine HUMINT. The reason is twofold. First, as emphasized here, they do not have organizational solutions. Second, they cannot be sensibly and responsibly treated in unclassified studies. Many similar issues for SIGINT, IMINT, and CI deserve serious leadership attention, but unclassified and open discussion of them will produce neither effective changes nor an adequately informed treatment of them.

CIA/DO relations with the FBI are dealt with more fully in the section on counterintelligence. Suffice it to say that the relationship has always been troubled. For several reasons this relationship deserves structural attention. First, in light of changed world circumstances and threats, it is increasingly likely that the FBI and CIA will collide in their activities overseas. A better understanding of their competing roles, responsibilities, and missions, and the structures that reflect them will therefore be important. Second, the CI relationship between the two agencies has long been cloudy.

The Ames case only brought to the public's attention turf boundaries and competing interests that are very old. Although the CIA appeared to be the problem and the FBI finally the solution in uncovering Ames, serious questions should be raised about how Ames could communicate with Soviet case officers in the

Washington area without the FBI becoming suspicious over such a long period. The Ames case is hardly just a CIA problem. It is also indicative of serious weaknesses in the FBI's CI operations.

Also, it should be noted in passing that the CI connections between the FBI and the CIA are only one side of a triangle. The CI operations of the military services are also related to both the FBI and CIA. Jurisdictional issues exist, particularly between the FBI and the military services, but also between the CIA and the military. They are more properly dealt with, however, in the section on CI.

Problems Inherent in Clandestine HUMINT Organizations

Leadership and management of clandestine services confront several unique problems. To some degree, a few of these problems are found in SIGINT and IMINT organizations, but with HUMINT, including CI, they take on special features. They present challenges to the management hierarchy that are not found in most bureaucracies, in the government or in the private sector. When members of the Congressional oversight committees have spoken of a need to change the "culture" in the CIA, they are talking about precisely these kinds of problems although they usually have difficulty in being specific about their causes. But they rightly perceive that there is something special about the nature of the problems. "Culture" happens to be a useful category to describe them because of its vagueness. In seeking successful remedies, however, it is essential to overcome that vagueness and specify more precisely the problems as well as their causes. Identifying a few key ones will help make the point.

First, deception and misrepresentation are the heart of clandestine HUMINT skills. Effective "case officers" must excel in the business of making appearances conceal realities. This is not only critical for their handling of agents; it is no less critical in techniques for recruiting agents. To put it colloquially, being good as "con artist" is extremely helpful in recruiting and handling agents. The same abilities are not helpful to managers and leaders in hierarchical organizations. If lower- and mid-level managers in bureaucratic structures have a proclivity for "con games" and "managing" the reporting of the cold, hard facts of operations both up and down the chain of command, that can be highly dysfunctional for the organization. In such cases, the top management levels are denied adequate information for controlling and directing the organization effectively toward its goals.

All intelligence organizations (and most military organizations), because of their secrecy requirements, confront this management problem, but clandestine HUMINT organizations have the greatest propensity to become afflicted by it. Skills honed for recruiting and handling agents are easily turned to dealing with undesired management pressures from above. Higher-level managers, a case officer can easily conclude, simply do not understand his problems in a particular case. Thus he can easily justify misleading the manager by believing that if the manager actually did understand, he would agree with the case officer. That means, of course, that a little deception in dealing with the superior is actually in the overall best interest of the superior. The complex human dimensions of handling agents encourage such reasoning. An agent, when he is recruited, is essentially placing his life in the case officer's hands. The case officer knows this and promises complete loyalty. When telling the unvarnished truth to management might be risking the

agent's life, or at least his well-being, the decision to divulge the whole truth is not easy. The moral dilemmas are enormous.

The problem does not stop at this point. As his career progresses, the case officer will be promoted to a management position. There he stands between case officers and higher management. The same old inclinations to play "temporary" games with the facts easily come into play. The problem repeats itself right to the top of any clandestine HUMINT organization. Moreover, as time passes, there is an accumulation of distortions from such behavior in what the top management knows about the operational levels. Occasional crises and flaps naturally arise that clear up some of these distortions when serious investigations are conducted, but the overall tendency is toward the accumulation of distortions.

Most experienced clandestine HUMINT managers are familiar with these problems, especially the problem of case officers becoming too attached to their agents and losing objectivity in judging their reliability and productivity. Still, the pressure to recruit agents exists, and the willingness to order that non-productive agents be dropped is mitigated. That climate also accumulates and undercuts management's control over operations.

The second kind of problem is related to the first, but it is different. The life of a case officer is difficult. He must work in anonymity. When he has a dramatic success, he cannot be rewarded by public recognition. He must live with a "bushel over his candle." Even his family cannot know. After ten or twenty years in the clandestine service, he is a gray and inconspicuous member of any community he lives in, and his children must see him that way. Suppressing one's ego, as this career requires, is not easy. To the extent it is gratified, it must be within the confines of the clandestine service. One is recognized for solid accomplishments only by one's peers and fellow clandestine officers. This climate creates a strong bonding effect. Loyalty to one's fellow officers becomes an overriding value. In principle, such cohesiveness contributes to operational effectiveness and useful collection, but in practice it can easily create a contradiction between the contributions by the clandestine service to the IC and the national security interest on the one hand and the informal group interests of clandestine officers on the other.

The clandestine service is not entirely unique in this regard. SIGINT organizations, IMINT organizations, and even analysis units must labor in anonymity to the outside world. They receive recognition primarily from their fellow workers. An indication of this social problem is reflected in a comment by several people about an individual who had performed an incredible feat in a technical intelligence collection operation. They called him "Top Secret Famous." That is, only a few people with Top Secret clearances in his department knew the extent of his achievement. Thus all intelligence organizations have this particular problem of coping with adequate recognition of performance and also retain the bounds of secrecy. In so doing, they inevitably create an informal internal cohesiveness that works against admitting mistakes and keeping the higher levels of management fully informed.

In HUMINT organizations, however, the problem is more acute. The personnel often work alone, away from peers who know their worth. And their skills that make them successful operators can easily be turned against their management. Coming from operational experience themselves, the managers are inclined to be forgiving.

A third kind of problem arises from the tensions between CI and offensive clandestine operations. The case officer wants his agent to succeed; he naturally wants to believe him. The CI officer is naturally distrustful of every agent. If the ethos of CI becomes too dominant, offensive operations will clearly suffer. And if the ethos of the primacy of offensive operations becomes too dominant, security will suffer. The history of the DO has been the swing from one kind of dominance to the other. James Angleton's paranoia as head of CI, if the open sources about his practices are to be believed, seriously hurt offensive operations. After his departure, the pendulum swung to the point where Aldrich Ames could survive as a Soviet and Russian agent for several years.

Fourth, clandestine services are confronted with a deadly problem if they suffer a serious high-level penetration by a hostile intelligence service. Once the penetration has been discovered and publicly acknowledged, how is the service to recreate the public image that it is free of such penetrations? This question must be answered for very practical operational reasons. Even if the service is entirely certain that it has eliminated the problem, its public image of being penetrated persists. A potential recruit in a target country, especially if he is well placed and informed, will know about the penetration. Can he afford to trust a case officer from that service to recruit him when he knows that the service has been penetrated? How can he be sure that, although one "mole" has been detected, there are not others? Unless he can be sure that there are none, he would be unwise to allow himself to be recruited.

The Ames case confronts the CIA with precisely this situation. CIA may clean up its internal problems and be entirely free of penetrations, but as long as the public image persists, it will be unable to recruit some of the most promising and high-level agents. Certainly there will be exceptions, but the climate of uncertainty, the image of the CIA being afflicted with a virus that can easily be fatal to an agent, will remain. Penetrations are extremely serious matters for SIGINT and IMINT organizations, but they do not face the same problem in recovering. This is a problem of special importance to clandestine HUMINT operations.

Considering Solutions to These Problems

The second problem, dealing with the requirements for recognition of genuine accomplishments and effective service by clandestine service personnel, is a management problem, not one that submits to structural solutions. It is somewhat less a problem in military HUMINT organizations because the personnel are mostly commissioned officers. They have rank that can be known to their families. When they retire, they can be honored with formal military ceremonies. The military simply has more instruments for dealing with this problem. Civilian HUMINT services face a more difficult challenge in this area.

The first problem, arising from the syndrome of clandestine operational skills affecting the flow of accurate and complete information up and down the management lines, has no easy solution. It, too, is a management problem, but a very special one. Two ethics are in conflict: the ethic of operational dealings with agents and the ethic of management integrity. The nature of the conflict in a clandestine service is certainly special, but variants of it are found in military organizations. Small groups form very tight social relations in military units, and loyalty to these groups frequently conflicts with the military units' missions and values. The most conspicuous examples, but by no means the only ones, are found in the cheating

scandals that occasionally erupt in the military academies. Honor systems in the academies have the practical purpose of socializing young men and women to place the institution's interests and values above their personal and small-group loyalties when there is a conflict. Military operations require that. When a military unit receives a combat mission order, that mission becomes more important than the life of any member of the unit. Its commander must be willing to risk lives to achieve it. This, of course, is the extreme case, but unless military organizations can sustain their priority of values, they will fail in their missions. The whole idea of an officer's "honor" and the code for an officer's behavior rests on the recognition that he must live and die by that priority of values. It is highly undemocratic, seemingly very unfair, but finally essential. And years of indoctrination are required to instill the ethic. Moreover, the ethic inevitably erodes over time and requires measures to revitalize it.

There may be a leadership lesson here for controlling clandestine HUMINT organizations, in dealing with the so-called "culture" problem. There is no intense socialization experience in the training of clandestine service officers of the kind found in the pre-commission training of military officers. It is also worth examining the military clandestine units for their experience in coping with the traditional problems of integrity in answering to the chain of command, recognition of achievements, and so forth. In principle, the commander of military HUMINT organizations has available methods for dealing with these problems that are absent from the DO.

Organizational Issues

If the recommendations for structural reform in the DCI's management capabilities are implemented, if NIMA is allowed to operate as an effective IMINT national collection agency, and if the NRO program offices support NSA and NIMA under their national-manager directors, all of these changes will have a large impact on the internal composition of CIA. CIA now consists of three major components, the DI, the DS&T, and the DO. The DI, of course, would move under the NIC and the DCI's direct control. A large part of DS&T consists of parts of the NRO. But it also contains elements that provide technical support to the DO, and it manages the Foreign Broadcast Information System. And it has a few other activities.

The proposed organizational changes would leave CIA with the DO as its primary and major component, but it would also retain a truncated DS&T. The implications of these changes are clear. CIA would become a HUMINT agency. Leaving the FBIS in CIA makes sense. FBIS is mainly an overt HUMINT collection effort. Its value extends far beyond the intelligence it provides. The American university and think-tank community is highly dependent on it for access to the media in countries throughout the world. It is extremely important to retain and support because, through the private sector research based on its products, the IC gains enormously in open-source political and military analysis.

Recommendations

- Restructure CIA, giving it two major components, the national clandestine service (NCS) and a component for handling overt HUMINT.

The director of this restructured CIA becomes the “national HUMINT manager.” His core responsibility, of course, is clandestine HUMINT and covert action, but he also must take responsibility for overt HUMINT. To the degree that he is knowledgeable of what HUMINT requirements can be answered through overt sources, he will be better able to target clandestine collection on those requirements that overt sources cannot meet. This kind of trade-off in allocating collection resources is analogous to the kinds of trade-offs the national managers of SIGINT and HUMINT would be asked to make.

- Retain a residual S&T capability in the clandestine service for support to HUMINT.

The DO requires considerable S&T support for clandestine operations. The capability to provide it, therefore, must be maintained at CIA. At the same time, some kinds of S&T support for CIA operations can and have been provided by NSA. Taking advantage of that source and others in the IC should be standard practice.

At the same time, CIA needs some S&T capabilities for a number of collection activities that depend heavily on HUMINT but also have a large technical character. Some are interagency in character, and that kind of interagency cooperative effort is absolutely essential to maintain.

The bureaucratic inclination for a CIA S&T organization will be to engage in “unnecessary originality,” inventing capabilities that already exist elsewhere in the IC. That is to be expected, but the DCI can limit its adverse effects by using his CMS Science & Technology section to stay abreast of the problem.

A frequent defense of the NRO and the present CIA/DS&T is that they have proven innovative, flexible, and able to field new technical systems rapidly, while similar endeavors within the military services have foundered on bureaucratic infighting and program delays. A few decades ago, this was a sound case. The Air Force probably would never have fielded the U-2 or the SR-71, and in no event would they have been fielded as rapidly. A lot has changed over the years, however. The concentration of strong technical skills in both NRO and CIA has declined. NSA’s record of rapid development in a number of areas has been impressive, and an effective NIMA could provide the innovation and momentum for fielding advanced IMINT collection platforms.

Finally, the kind of S&T section prescribed in the CMS for the DCI would provide a mechanism for virtually unconstrained innovation in “skunk works” programs. The residual S&T capability in CIA also provides an option for the CMS S&T section to use in these endeavors. In other words, with the changes recommended for R&D management by the DCI, there would be mechanisms for a renewed R&D vitality in the IC that has abated over the years in the NRO and CIA.

- Formally establish an OPCON relationship between the CIA/DO (NCS) and the military clandestine HUMINT elements analogous to NSA’s relationship with the military SCEs.

This means making the DO truly take charge of military clandestine HUMINT, treating it as an adjunct to its own efforts. This would mean a much deeper involvement by the DO in directing and supporting military clandestine operations. The change actually requires no new formal authorities for the DO. The DO’s

present coordination and approval authority over military clandestine operations gives it as much involvement in them as it desires to have.

Certain tensions could result from this change, but they need not. If the DO attempted to allocate military capabilities wholly to non-military collection requirements, ignoring military needs, the Joint Chiefs would object. The DO has long accepted, somewhat ambiguously, a commitment to meet military requirements, but in practice, it has never devoted serious resources to them. As one example—from the Cold War and now no longer a requirement—U.S. forces in Europe needed a plethora of low-level agent support in then-communist Eastern Europe. The CIA never had the resources to begin to meet them, and that was one reason for retaining Army clandestine HUMINT. With those capabilities (now in DHS) under the OPCON of the DO, it would be much better prepared to deal with such requirements. Likewise, in the Persian Gulf War, similar requirements existed but the CIA was without assets to meet them. Had the CIA taken OPCON of the Army's ISA and other capabilities in the early 1980s, it could have created those assets without harm to its other non-military requirements.

One can make a strong argument for the abolition of all military clandestine capabilities. For that argument finally to be persuasive, however, the DO would have to be placed under the OPCON of the Secretary of Defense and of the Joint Chiefs. Otherwise, the experience of the military during the Iran rescue mission would be the norm. No HUMINT support would be forthcoming, and the military could do little about it. The alternative, therefore, is for the DO to take seriously its authorities and potential for managing military HUMINT.

- Allow the CIA/DO to retain its status as the covert action agency, but make it dependent on the Defense Department's capabilities for the conduct of any paramilitary covert actions.

The need for covert action in general and paramilitary operations in particular is not very large today. It would be unwise, however, to abandon entirely the maintenance of those options for the future. The clandestine HUMINT service, of course, is in by far the best position to manage such operations. The political and military intelligence required for the context of covert actions makes that true. At the same time, the DO is unlikely to match the depth of skills and capabilities for paramilitary operations that can be maintained by the military services. Those capabilities now have their own unified command, U.S. Special Operations Command (USSOCCOM). In peacetime, there is no practical reason why task-tailored complements of special operations forces cannot be passed to the DO's direct control on a case-by-case basis for actual employment. It has been done on a partial basis before. It makes good sense, therefore, to shift the responsibility for creating paramilitary forces entirely to the military services while leaving their peacetime operational employment to the DO. The objections by the Secretary of Defense on political grounds are understandable, but they should not be the deciding factor. The past record contains too many amateurish CIA paramilitary operations.

- Take a broad approach to designing and implementing CIA management of overt HUMINT.

It is easy to suggest that CIA, as the national HUMINT agency, take charge of the highly fragmented and poorly managed exploitation of overt HUMINT. It is another thing to be specific about how that should be done. The first problem is finding a practical definition of what is to be included as overt HUMINT. The

definition could be expansive, involving all the open media. Clearly CIA cannot take charge of reading the newspapers for policy-makers and military commanders; nor can it watch CNN's battlefield reporting for them. Prisoner of war interrogation units in the Army could conceivably fall under CIA OPCON. Many Defense Department de-briefing programs might also. Embassy diplomatic reporting can hardly be the management responsibility of CIA. Military attaché reporting might well be. These examples suffice to make the point: overt HUMINT collection is a burgeoning area whose management has long been neglected. It needs a disciplined management review which draws practical lines around what is to be included, what is to be excluded. And it will need to work with the NIC and the DI in order to distinguish between what is "collection" and what is already fit to be treated as "finished analysis." For example, some academic works and contract studies are "finished analysis" while open-source publications that do not provide finished products for answering specific requirements would be items for "collection."

As mentioned in the first recommendation above, an important result of better management control of overt HUMINT collection is that it can show the DO what not to collect through clandestine means. At present, the IC has no system for even considering how to determine this, much less accomplishing it.

- Address the CIA/DO "culture" and related problems with a wide range of management, leadership, and organizational reforms, including consideration of disbanding the DO and creating an entirely new clandestine service.

This recommendation is intentionally vague. The "culture" problems and their causes have been identified in general terms. Here, remedies must remain equally vague because open discussion of them is not useful. Moreover, the best remedies may not be obvious, and in some cases, they clearly are not. No outside study and set of recommendations can provide precise or complete answers. The most that can be done is to raise issues that make the depths of such problems apparent and thereby to provoke creative and imaginative thinking about possible solutions. Such ideas should go as far as consideration of the full dissolution of the present DO and a new start from scratch. Retiring the old name "Central Intelligence Agency" should also be considered, in order to give the HUMINT service a new name to emphasize the fresh start and cultural change.

Some members of the advisory committee for this study strongly favor the dissolution of the clandestine service, asserting that the value of its collection activities have always been marginal. Others favor dissolution of the present CIA/DO and the creation of an entirely new clandestine service in order to assure that no residual hostile penetrations like Ames or Nicholson remain, and to deal with changing the DO "culture." Still others would leave the DO to reform itself and to retain the "CIA" label after the DI and DS&T have been removed, altered, or dissolved. All three approaches deserve serious consideration.

Conclusion

Some aspects of this review will meet serious objections from CIA. Others will be dismissed as not essential. One or two may be welcomed. The negative reactions should be met with skepticism yet understanding. If the whole set of recommendations were implemented, the CIA, as it has existed to date, would become a thing of the past. It would lose its grip on the DCI. It would lose its leverage on the SIGINT and IMINT

budget with the dissolution of NRO. Finally, it would no longer have the DI. These changes would be initially viewed as amounting to the abolition of the CIA.

On the other hand, the clandestine service would stand to gain a great deal. Its operational control of military clandestine capabilities could double its resources and greatly extend its reach. It would be much better positioned to have cooperative relations with the military services. Its access to Defense Department paramilitary capabilities would vastly improve its operational capabilities while allowing it to avoid the recruiting, training, and equipping of such forces. The potential for exploiting overt HUMINT collection would be improved and possibly open a number of new programs and operations.

The recommendation that the DO's "culture" problems be subjected to some fairly far-reaching management changes would be met with stubborn resistance. For the serious long-term interest of the clandestine service, however, that reaction would be a profound mistake. The DO has many accomplishments in its record, and its present and former members are justly proud of them. They compose as gifted and talented a group of people as there is in the government. The sacrifices and risks they have made and the dedication to duty they have shown deserve our highest respect. All that said, however, events have dealt the CIA a series of blows that approach its limit to survive.

The damage began with the Congressional investigations in the mid-1970s, and has continued with embarrassing disclosures in steady succession ever since, right down to the Ames and Nicholson cases. To break this succession and to begin a genuine revitalization of the clandestine service, more than modest changes will be required. They must be so dramatic, so radical, that they inspire a new sense of confidence based on compelling and demonstrable evidence.

For example, the occasion of major restructuring in other parts of the IC provides an excellent opportunity for the CIA to go far beyond moderate internal reform. Can the record of episodes, including the Ames and Nicholson cases, ever be entirely washed away from CIA's public image? Not likely. Why, then, does it not make sense to take the occasion of IC-wide reform and formally drop the "CIA" name and label? It could be abolished to symbolize publicly the depth of change it was undertaking. A new incarnation, marked by a new name, has much to be said for it—if indeed it is accompanied by the kinds of fundamental reforms recommended here. Finally, can a clandestine service that has suffered a penetration of the kind that the Ames case represents fail to consider a virtual dissolution and a rebuilding from scratch? A professionally serious assessment of the situation inexorably pushes one toward that remedy.

Can a service that refuses to consider this degree of reform expect to be looked upon as truly professional? The first objection can be anticipated: but we cannot possibly survive several years of transition without a clandestine service, and it would take several years to implement such a radical remedy. The answer to this objection is twofold. First, now that the Soviet Union is gone, we have a few years of reprieve in which to carry out just such a remedy. Second, more than a few intelligence officers have raised serious doubts about how necessary a clandestine service is in the present era of voluminous publicly available information from an ever growing set of sources. The authors of this study are not fully persuaded that the United States can do without a clandestine service, but now is an excellent opportunity to test for a short time what would be lost without one.

The advisory group for the study was split on this issue. One member preferred the complete dismantling of the clandestine service. Several others agreed but favored erecting an entirely new follow-on clandestine service. Only two members favored keeping the CIA label and the present clandestine service. All agreed that the CIA (or its successor) should no longer constitute more than the clandestine HUMINT service. Although a full consensus was lacking for any single solution, there was a strong consensus for far more fundamental change than has been contemplated by any other intelligence reform study. Lesser reform measures will inevitably allow the present clandestine service to fall short of being first-rate and probably to continue to decay.

Note

1. See John M. Newman, *JFK and Vietnam: Deception, Intrigue, and the Struggle for Power* (New York: Time Warner, 1992), for a well-documented account of this example.

Section VIII

Counterintelligence

Introduction

Reforming counterintelligence (CI) is probably the most challenging of all the intelligence reform issues. CI is the most arcane and organizationally fragmented, the least doctrinally clarified, and legally and thus politically the most sensitive. Several recommendations for reforming CI in the Defense Department have already been made, and they will not be repeated in this section. They are fairly straightforward. Moving to the national level, reforming CI within the overall Intelligence Community (IC), things are not so straightforward.

For this reason, both the analysis in this section and its recommendations should be read as exploratory and tentative. The recommendations are assumed to be attainable within current legal operating authorities and constraints. Professional CI officers may disagree with some of the points made, but it is hoped that they will consider them seriously in any case. Where they are seen as challenging the conventional wisdom and practice, they may seem off the mark, but the record of conventional wisdom, and especially its practice of late, has not been exemplary. A challenge to both, therefore, is overdue.

Doctrinal Assumptions and Their Ambiguities

As in the other sections of the study, we begin with the doctrinal assumptions set forth in the “Principles and Concepts” section. Counterintelligence, it will be recalled, is defined as intelligence gathered about an adversary’s intelligence activities and capabilities. In other words, the CI function is no more than collecting information to unmask adversarial intelligence operations and capabilities. This is an important definitional boundary because CI is often also understood to include far more, specifically the “security” function involving specific types of action. Yet as the “Principles and Concepts” section made clear, security is a “command” function in the military and a policy-management function in civilian agencies. CI provides the information on which military commanders and civilian agency managers should base their decisions on which security measures to take, but CI officials do not have the administrative or command authority to promulgate security policies or to direct security measures. They do, of course, have that responsibility within intelligence organizations, and it includes access to intelligence information by individuals in other agencies. In other words, authority to grant security clearances for access to specific intelligence belongs to the DCI even for individuals outside the IC in user organizations. Beyond this authority, which is really to protect IC intelligence, not to provide general security to outside organizations, IC officials have only the power of persuasion about security measures in non-intelligence organizations.

This analytical distinction, setting CI apart as purely intelligence and not a security measure, has other ambiguities in practice. "Deception operations" are an example. Valid and comprehensive CI is imperative for operations intended to mislead an adversary. CI organizations obviously are in the best position to carry out some aspects of deception operations. Thus they become involved in operations that exceed the narrow definition of CI. Deception operations, however, like security measures, are command and management functions, not CI or intelligence functions.

Another ambiguous case for a sharp doctrinal boundary on CI is encountered in the neutralization of hostile intelligence operations. Within its own ranks and installations in the United States, the military services have the authority to arrest U.S. military personnel working for hostile intelligence services. Beyond U.S. territorial borders this authority is more extensive for the military services, but in the United States the military services cannot arrest hostile intelligence agents, either U.S. citizens or foreigners outside military installations. Only Federal and local law enforcement agencies can do that. Thus military CI is inexorably entangled with the FBI and sometimes other civilian law enforcement agencies if arrests and prosecutions are attempted.

Further complications for neutralization of agents concern the admissibility of CI as evidence by a court of justice. An agent can be exposed and accused, yet the evidence of his or her activities may not be admissible in court unless it is gathered with that purpose in mind. That can be costly; it can delay the neutralization of an agent, and it can seriously affect CI operations.

At that same time, as a law enforcement action, neutralizing an agent normally differs considerably from identifying and arresting an ordinary criminal. Criminals' motivations and modes of operation can be quite different from those of hostile intelligence agents. Criminal law enforcement methods overlap with CI methods, but they differ in fundamental ways. Mixing the two functions in one organization, therefore, raises serious problems; sometimes the two are incompatible. The example of the Naval Investigative Service handling the case of the Marine, Clayton Lonetree, in the American Embassy in Moscow is one unfortunate case mentioned earlier. Moreover, if we take a longer view of the FBI's record, to include dealing with Soviet espionage during and after World War II, especially in light of the opening of the Venona files and the recent book by Klehr, Haynes, and Firsov, based on newly available Soviet COMINTERN documents [1], one is struck by the ease with which Soviet intelligence evaded the FBI's CI efforts. Neither the FBI nor the Justice Department could cope with the disinformation and public campaigns inspired by the American Communist Party to blunt investigative efforts against Soviet agents. Nor can one argue that things have improved in the last three or four years in light of the recent Ames and Nicholson cases. That Ames could make "dead drops" and deal with his KGB handlers in Washington for several years undetected says as much about the weakness of FBI CI capabilities as it does about CIA's security practices. The CI operations of a law enforcement agency will predictably receive less support and prominence compared with that organization's law enforcement operations. The politics of fighting crime and the support for budgets in the Congress both favor law enforcement over CI operations. Equally important, organized crime does not have the skills and resources available to a state-backed hostile intelligence service. Thus criminals are easier to catch than spies, and quantitative measures of success, i.e., number of criminals apprehended versus number of spies caught, will always tend to make law enforcement look better than CI operations.

A further complication arises for CI where double agents are used. They can be excellent sources for CI. At the same time, neutralizing them can be done entirely by CI organizations without any law enforcement involvement. Such operations, however, go beyond CI defined as only the collection of intelligence about hostile intelligence operations. They are in effect “security” measures that CI operators take on their own, normally with consulting military commanders and civilian managers of the organizations they support. They also raise the important question of who decides whether and when to prosecute a hostile intelligence agent, as opposed to other possible responses.

Finally, CI is extremely important as support for intelligence operations, especially HUMINT operations, but also SIGINT and IMINT. A clandestine HUMINT service finds an organic CI capability virtually imperative. At the same time, CI capabilities organic to clandestine HUMINT services will inevitably be relegated to secondary priority vis-a-vis offensive HUMINT operations. When that is not the case, and when CI is given first priority, there is a risk of paralyzing offensive HUMINT. We have witnessed examples of both imbalances in the CIA/DO. During James Angleton’s time as head of the DO’s CI, it seems that CI’s priority became counterproductive for offensive HUMINT. More recently, with the cases of Ames and Nicholson, CI appears to have been given too little priority.

There is no clear way to define the CI function that obviates some of these ambiguities, but there are ways to mitigate a few of them. Adhering to the doctrinal points about CI explicated in the “Principles and Concepts” section does not remove the ambiguities and related problems, but it does highlight them. Unless they are highlighted, the problems they cause tend to go unaddressed. We will, therefore, stick with the narrow doctrinal definition of CI.

Problems and Solutions

Most, but not all of the problems with CI as it is now performed in the IC, have been illuminated in the foregoing analysis. Only two, however, are amenable to structural reforms—(1) the mixing of CI with law enforcement and (2) the mixing of CI with offensive clandestine HUMINT.

The first, mixing CI and law enforcement within a single agency, can be readily solved within the Defense Department. The Navy and the Air Force need to create independent CI organizations on the model of the Army’s CI structure.

At the national level, however, the matter is not so simple. Applying the same principle there would require the removal of the CI function (investigation, and also probably arrest) from the FBI. The bureaucratic opposition to this solution would be, to say the least, monumental. Assume, however, that it could be overcome. What alternative arrangement might be preferable? Following the “Principles and Concepts” doctrinal guidance, the answer would be to create a “national CI manager” with an independent organization, but still operating within currently accepted legal limits. There are precedents for this approach. The British MI-5 organization roughly approximates it.

To apply the “national manager” concept would also be to give that manager not only his own autonomous CI organization within the IC and under the DCI, but also to give him OPCON, or at least “coordinating authority,” over all other CI, especially military CI but also CIA’s CI. This is a somewhat larger domain of CI responsibility than the British MI-5 has.

The national manager approach would also require that the national CI agency be responsible for the dissemination of relevant CI for all civilian and military organizations to support their security operations. This corresponds to the national SIGINT, IMINT, and HUMINT managers’ responsibility to provide support to users at the national and the tactical military level. If the CI is not provided directly to the civilian or military organization, then it should be sent through organic CI organizations within the military and elsewhere reinforced by the national CI organization.

This kind of broad support responsibility would be a huge cultural and operational change. The FBI jealously guards its coordinating authority over the military CI operations in the United States but provides absolutely no CI support to the military services. Nor does it have a record of great CI support to the CIA. Fulfilling this responsibility would require a communications structure dramatically different from anything the FBI has ever contemplated, much less understood.

Beyond the CI support function, the FBI has no experience in military CI operations or any idea of military CI needs. It would have to become much immersed in a radical transformation of its mission and concept of operations. Given the FBI’s domestic law enforcement mission, the FBI culture would be virtually impossible to transform in this way. That means that a separate national CI organization is essential for any significant improvements.

At the same time, it should be recognized that a new organization would face an enormous challenge in coping with an effective “national manager” role. Deep mutual distrust, long extant in the CI community, is one obstacle. The idea of providing national-level support to lower organizational levels is new, and most CI officers would not easily understand or accept it. Several other difficulties of this sort would be met, but they are not an argument for not making this structural change. Rather they are evidence of how urgently the change is needed.

The second major reform of CI falling under the doctrine of this report is resolving CI and HUMINT collection organizations. Creating a national CI organization obviously raises the question of what would happen to CI activity within CIA/DO. It probably could be somewhat reduced, but it could not be transferred entirely to the national CI organization. Some degree of OPCON over CIA’s CI would be in order, but total control would not be appropriate, any more than would be total control over military CI.

A national CI organization, however, would have to have enough OPCON over and access to all CI operations and production to provide the national CI manager with a total view of CI holdings, CI operations, and CI user needs. And it would have to know enough about other CI efforts to be able to decide what additional CI could and should be supplied to these users.

Developing effective OPCON and CI support procedures will not be easy, but it must be done if the advantages of a national CI organization are to be realized. Moreover, the enormity of this challenge is an

index of the weakness and inadequacy of the present CI organizational structure. When this is understood, it should occasion no surprise that Soviet and Russian intelligence operations defeat it in spectacular ways. Quite the contrary; the weakness of U.S. counterintelligence raises suspicions that it is being defeated in many other cases yet undetected.

Security, Deception, and Agent Neutralization

Avid proponents of more effective CI are often inclined to try to solve security, deception, and agent neutralization problems, especially the security problem, by structural changes, mainly by advocating placement of the security function on CI and other intelligence organizations. That tendency was publicly evident in the 1980s when it became widely known that the U.S. embassy in Moscow was heavily penetrated by technical devices. The CI effort that disclosed the penetrations was finally done by a non-CI organization. The task of neutralizing the penetrations and restoring security could only be the Secretary of State's. His department "owns" the embassy. Neither the CIA nor the FBI nor any other IC component has directive, managerial, or command authority over embassies. That means, therefore, that restoring security after CI disclosed the penetrations could rest only with the Department of State. Considerable struggle and bureaucratic infighting followed for several years thereafter in which a number of people—within Congress and the IC—tried to place the security cleanup responsibility on IC organizations. The IC certainly needed to assist it, but could not lead and direct the operation.

The attitude and its underlying misperceptions, confusions, and mixing of the CI and security functions persist in the IC and elsewhere. The intention is commendable, but the solution of structurally uniting CI and security functions is not only wrong but downright counterproductive. The State Department, under attack from other agencies and Congress about the penetrations in Moscow, became defensive and more reluctant to take aggressive remedial measures than it might have otherwise. The lesson was clear in this case as in numerous similar cases. Intelligence organizations, especially those which produce CI, can deliver the information they collect and analyze to commanders, policy-makers, and managers affected by that intelligence, but they cannot make these users act on it. If the Secretary of State is indifferent to having his cable traffic read by foreign intelligence services, neither the DCI nor any of his agency heads can force him to change his attitude. This is not an IC structural problem. Neither is it an IC policy problem. It is the President's leadership problem, a matter far beyond the limits of a study of the IC.

Where hostile intelligence operations penetrate IC components, of course, that is an IC security responsibility. The Ames and Nicholson cases indeed concern the DCI and CIA/DO. As has already been suggested in the HUMINT study section, security measures to defeat penetrations at that level require structural changes, extremely radical ones.

The complete disbandment of a clandestine HUMINT organization has to be considered once it has been seriously penetrated. Policy changes can never really be sufficient because the most promising high-level foreign officials for that HUMINT organization's recruitment would be extremely unwise to allow themselves to be recruited if they knew penetrations had occurred. The best potential recruits will avoid working for such a contaminated clandestine service, just as they would avoid contact with persons known

to have an incurable infectious disease. Of course an “infected” clandestine service will continue to succeed in recruiting spies—that is why infectious diseases spread—but it will never know what potential agent has decided not to risk being recruited, and the organization will never know if it is really healthy again.

This diagnosis and the prescription, of course, fall under the security function, analogous to the way KGB penetration of the U.S. embassy in Moscow did. It is a management/leadership problem, not an intelligence problem.

Deception, like covert action (CA), goes beyond intelligence although intelligence plays a critical role in developing deception operations. Excellent CI is the prerequisite for any serious deception operation, a reason for building a highly effective CI capability, but not an issue for IC structural reform.

Neutralization of an agent, short of arrest or some other open and direct means, can be accomplished, at least temporarily by feeding misinformation. This raises a policy issue: is such an operation CA? Or is it deception? The answer has to be “neither.” Misinformation is a CI instrument unless it is part of a much larger operation that unambiguously qualifies as CA or deception. CI operations must be allowed some latitude in narrow, single agent cases; that is, they should be able to neutralize an agent by clandestine means as a legitimate action within purely CI operations.

Other Issues and Problem Areas

CI and clandestine HUMINT sometimes conflict. CI has been and remains primarily a clandestine HUMINT activity in most of its operational methods. This has led to the FBI actually competing with the CIA/DO in the offensive HUMINT area. Some of this may be unavoidable. How far to let it go and when to pull CI organizations back from such competition is a management and policy issue, not an issue for this study.

Counterintelligence should make use of all the collection disciplines. CI operations can be greatly enhanced if they are supported by SIGINT, IMINT, and other technical measures. Although this is fairly widely understood, carrying it out in practice is not so easy. Aside from clandestine HUMINT, CI operations people do not tend to be highly knowledgeable of how the intelligence collection disciplines work or what they can do to enhance CI operations. Nor do the specialists in SIGINT and IMINT always know how they can help CI. This, however, is not a structural problem. It is a policy and operational methods issue, and therefore, beyond the scope of this study.

Multi-discipline CI deserves noting, however, because it has structural implications. Law enforcement agencies with CI responsibilities lean toward technical means used for law enforcement, but these are not nearly as broad in their scope and potential as a truly multidisciplinary CI methods. The same is true for CI operations lodged within clandestine HUMINT organizations. The implication of these observations is that an autonomous CI organization, even without altering existing legal rules, is probably better positioned and easier to interest in exploiting other disciplines. Reshaping the thinking and operational outlook of CI

personnel, however, still requires strong management emphasis. No structural change alone will ensure that it happens.

The relationship between CI and law enforcement is complex. CI, of course, has to be highly informed about legal issues in a number of areas. First of all, it must not just gather accurate CI; it must do so with regard to legal rules which vary, depending on the who, when, where, and why of its use. This problem is as delicate as it is complicated. For example, it must consider whether or not that information can be used in legal prosecutions where CI uncovers hostile agents. And it must be concerned with the potential damage to CI, and other intelligence operations that use CI, that may be caused by prosecutions. There are also numerous additional legal considerations beyond the scope of this discussion.

On the opposite side of the concern about apprehending and prosecuting hostile agents is a different issue. Putting off, even disallowing apprehension of an agent long after adequate evidence for prosecution is available can sometimes yield great CI results, i.e., obtaining much more information about a hostile intelligence service's capabilities. Running these kinds of operations is expensive, not only in funds but in personnel resources. Law enforcement agencies understandably do not favor them. Purely CI organizations are far more likely to want to pursue them. This reality is yet another strong reason for an autonomous CI organization. For it to reach its full operational potential, the CI operators will have to cultivate a mindset that differs somewhat from the law enforcement mindset, even though a decision whether or not to treat a matter as a potential criminal investigation must always involve law enforcement authorities.

Another critical issue for CI is protection of individual rights of American citizens. CI and SIGINT both are subject to stepping over the line when individual rights are involved. A CI organization, therefore, has to be well supported by qualified lawyers who can police this boundary, alerting managers when the dangers of crossing it are imminent.

The public reaction to the creation of a national CI service is likely to be negative unless all of these legal considerations are carefully and effectively addressed. If they are not, then a CI organization simply cannot be effective and gain the required public and Congressional support needed for its long-term existence.

A comprehensive picture of our own CI is necessary. Any intelligence organization tends to be inward-looking and mistrustful of cooperation with other intelligence organizations, even in the same government. The public record on this point includes the intelligence services of the Soviet Union, Germany during World War II, France, Britain, and others. The United States, of course, has not been an exception, especially in the HUMINT and CI disciplines. Clandestine HUMINT operations can produce important and useful intelligence without it providing a comprehensive picture of an adversary's military and foreign policy. This is much less true for CI. A CI organization can be tied up by an adversary through double agents and other feeds of information in a way that allows it to produce what appears to be effective CI without knowing that it is being seriously misled. The only way a CI organization can defeat an effective counter operation of this sort is by having a total and comprehensive view of all CI efforts within its own government. Compartmentation and fragmentation of CI structures make a government's CI capabilities highly vulnerable.

To defeat an adversarial strategy it is essential to have a comprehensive and total view at the top. In other words, a strong analytical effort at the national level based on authority to peer down into the many compartmented CI operations can detect a hostile intelligence service's operational games. The present IC structure for CI is highly fragmented. There is little tradition of sharing at the top to create a comprehensive view for all CI. Periodically, major attempts have been initiated by DCIs, and the CIA/DO chiefs of CI have occasionally worked hard at achieving such cooperation, but these developments have always been short-lived, never fully institutionalized. The FBI's independence and turf-consciousness in this regard are notorious among the military services' CI operators. And the turf wars between the FBI and the CIA have sometimes been described in memoirs by retired agents and books by outsiders about both agencies. The DCI's several innovations, e.g. an IC Counterproliferation Center, Counter-Drug Trafficking Center, etc., have in no sense overcome these obstacles, although they may be masking some of them.

This problem may have no full solution, but clearly structural features of the present CI organizations in the IC make it much worse than it has to be. Creating a national CI service is about the only way to make significant progress in mitigating, if not fully eliminating, this problem. Inter-agency cooperative efforts simply will never have the power to overcome the turf barriers dividing the present set of CI organizations.

CI training and education are also grossly neglected areas. Unlike SIGINT and clandestine HUMINT, CI has no consolidated training and educational program. Several programs exist within various CI organizations, but even those are spotty, often given secondary priority. Clandestine HUMINT skills are often considered all that is really necessary for training CI officers. The training area, therefore, is afflicted with serious structural deficiencies.

Among the most important materials for teaching CI officers effective operational and analytical methods is the historical record of all past CI cases. Yet such compilations are largely non-existent. Partial ones probably exist in some CI organizations, but the FBI and CIA have no tradition of gathering, collating, and synthesizing the CI cases of the military services. And if they do that for their own CI cases, they never make these files available for training military CI officers.

For CI officers to acquire more than rudimentary operational competence, the historical files of all cases on targets of responsibility are clearly essential. This is obviously true for CI operations, but it is also true for CI training courses and mid-career development education. A national CI school, therefore, would seem to be an essential and elementary step toward building a serious and professional counterintelligence service in the IC. Today it does not exist.

Recommendations

The many CI problems and issues mentioned above are by no means a comprehensive list. They are merely the most obvious, serious ones. Still, they present a disturbing picture of CI as a fragmented, poorly coordinated, and often amateurish discipline within the IC. Several, of course, are policy and management problems, but a number of others cannot be adequately addressed without structural changes.

At the same time, precisely what structural changes would be best to implement is admittedly debatable. Using the "Principles and Concepts" section as a guide suggests some solutions, but ambiguities remain

concerning the close connections between CI on the one hand and law enforcement and clandestine HUMINT on the other. Similar ambiguities also remain when the non-CI functions are considered, namely security, deception, and CA.

These concerns notwithstanding, giving CI an independent organization at the national level that separates it from law enforcement and clandestine HUMINT appears to be imperative if significant improvements in CI are to be made. To launch this major structural reform, the following recommendations are made as the minimum:

- Create a National Counterintelligence Service (NCIS).

The FBI's CI department can form the core of this organization, and it can be augmented with small elements from CIA's CI organization.

- Designate the Director of the NCIS the "national manager for CI," responsible to the DCI in the same way as the national manager for HUMINT.
- Give NCIS "coordinating authority" over all CI operations within IC components.

Whether or not this authority should include operational control (OPCON) over all, or part, of CI operations in other IC components should be determined by experimentation and practical experience.

- Give the national manager for CI responsibility for providing CI support to all departments and agencies at the national level. As with OPCON, experimentation with the national manager assuring CI support to tactical military units should also take place.

Just as the national managers for SIGINT, HUMINT, and IMINT are responsible for linking national collection assets to support for tactical military operations, the national manager for CI can probably usefully link certain kinds of CI support to augment and strengthen organic CI capabilities in tactical military organizations.

- Make the national manager for CI responsible to the DCI for maintaining a comprehensive CI picture of all relevant CI target foreign intelligence services.
- Direct the national manager for CI to create a CI school and ensure that it has available the record of all CI cases as its primary instructional material.
- Retain a significant organic CI capability in the CIA/DO and the military services, giving the national manager for CI access to these activities for coordination purposes.

The recommendations for CI reform made in the section of this study on Defense Department intelligence are not only complementary with the foregoing recommendations but are necessary to implement several of them.

Note

1. Harvey Klehr, John Earl Haynes, and Fridrikh Igorevich Firsov, *The Secret World of American Communism* (New Haven, CT: Yale, 1996)

Section IX

Conclusion

The foregoing analysis has been highly critical of many aspects of IC structure and operations. Some of the criticisms are well known, others much less so. The entire set is far from exhaustive, but it provides a fairly comprehensive appreciation of the sources of most of the serious problems in the IC over the past decade. It has also explained why many problems derive from misalignment of intelligence output responsibilities and resource input authorities. This reality entangles several of the structural problems in ways that make partial solutions virtually impossible. Let us, therefore consider appropriate sequences for IC reform, what must be done concurrently, and what can be done at any time.

The imperative starting point for reform is disestablishing the NRO as an autonomous agency and making its program offices turn to the national managers of SIGINT and IMINT for funding rather than to the Congress. That is the *sine qua non* for moving to a system of “national managers” of the collection disciplines. And without such a system, the DCI has little chance of applying PPBS principles efficiently to the National Foreign Intelligence Program. As long as the DCI cannot do that, he cannot explain his program effectively either to OMB or to the congressional oversight committees, and he will have only limited influence on resource allocations within the IC.

Once the DCI has national managers for the collection disciplines, he will find it imperative to build a more effective Community Management Staff. And to the degree he does this and begins to introduce more rationality to the NFIP, he will inevitably have to shift his center of operations to the entire IC, devoting less attention to his second “hat,” Director of the CIA.

Such changes in how the DCI manages resources will also push the DCI toward a different approach to managing intelligence production throughout the IC, as well as for national (particularly White House) use. The DCI will have to pay more attention to the amount and types of intelligence output—intelligence products that are actually used—as a guide for executing his program management responsibilities. To the degree he does this, he will find the present large CIA/DI not very cost-effective. And he will want a staff organ and an analytic capability that can range throughout all the intelligence production units in the IC. The NIC, supplemented with a relatively small analysis unit, is a logical way to satisfy this need.

All of these changes should be made more or less at once. They are mutually related and therefore cannot be effectively staggered over a long period. They go together or not at all. The DCI must have full support from the Secretary of Defense, especially concerning the dissolution of the NRO and making the CIA/DO the national manager of HUMINT.

Reform of the internal DoD intelligence structure could go forward independently, earlier or later. While the DCI can encourage it, the Secretary of Defense must implement it. The DCI cannot.

Reform of counterintelligence can also be done more or less independently, but when it is begun, it must include reforms in both DoD CI and CIA CI.

Depending on the approach one chooses in reforming the HUMINT discipline, especially clandestine HUMINT, the task will be quite large and traumatic, or relatively smaller but still rather traumatic. It should not be attempted, however, until the system of national managers of the collection disciplines is established. The national HUMINT manager's responsibility for DoD HUMINT will then make significant change essential. If the national HUMINT manager's attitude toward DoD HUMINT is not dramatically altered from the traditional CIA/DO attitude, no real progress will be achieved.

Such are the considerations for sequence of reforms. A few can be done independently, but the most important ones tend to be linked to several others which must be accomplished concurrently. The largest fiscal savings will come from the national manager system and the dissolution of the NRO. They can be implemented by Presidential Executive Order and thus do not require legislation. In fact, all can be done by Executive Order, except the creation of a National CI Service. That requires congressional action.

Finally, effective IC reform will only be carried out when a rather narrow but high-level constituency decides to demand it. This constituency includes the President, the Secretary of Defense, the Secretary of State, and the leadership of both parties in the House Permanent Select Committee on Intelligence, the Senate Select Committee on Intelligence, and probably also in the Senate Armed Services Committee and the House National Security Committee. There is one important exception. If a National CI Service is to be created, a much larger constituency will be essential, one that can assure the public that U.S. citizens' civil liberties are in no way endangered, and one that can cope with the FBI's objections. Both are daunting challenges, but given the impending clashes that are bound to occur between the FBI and the DCI as the FBI increases its collection activities abroad, they may prove easier to confront earlier rather than later and with much less international embarrassment to the United States.

In any event, the reform challenges in the IC are large, and as facing up to them is delayed, the costs to the taxpayer increase, and reform will become all the more complicated and seemingly intractable.

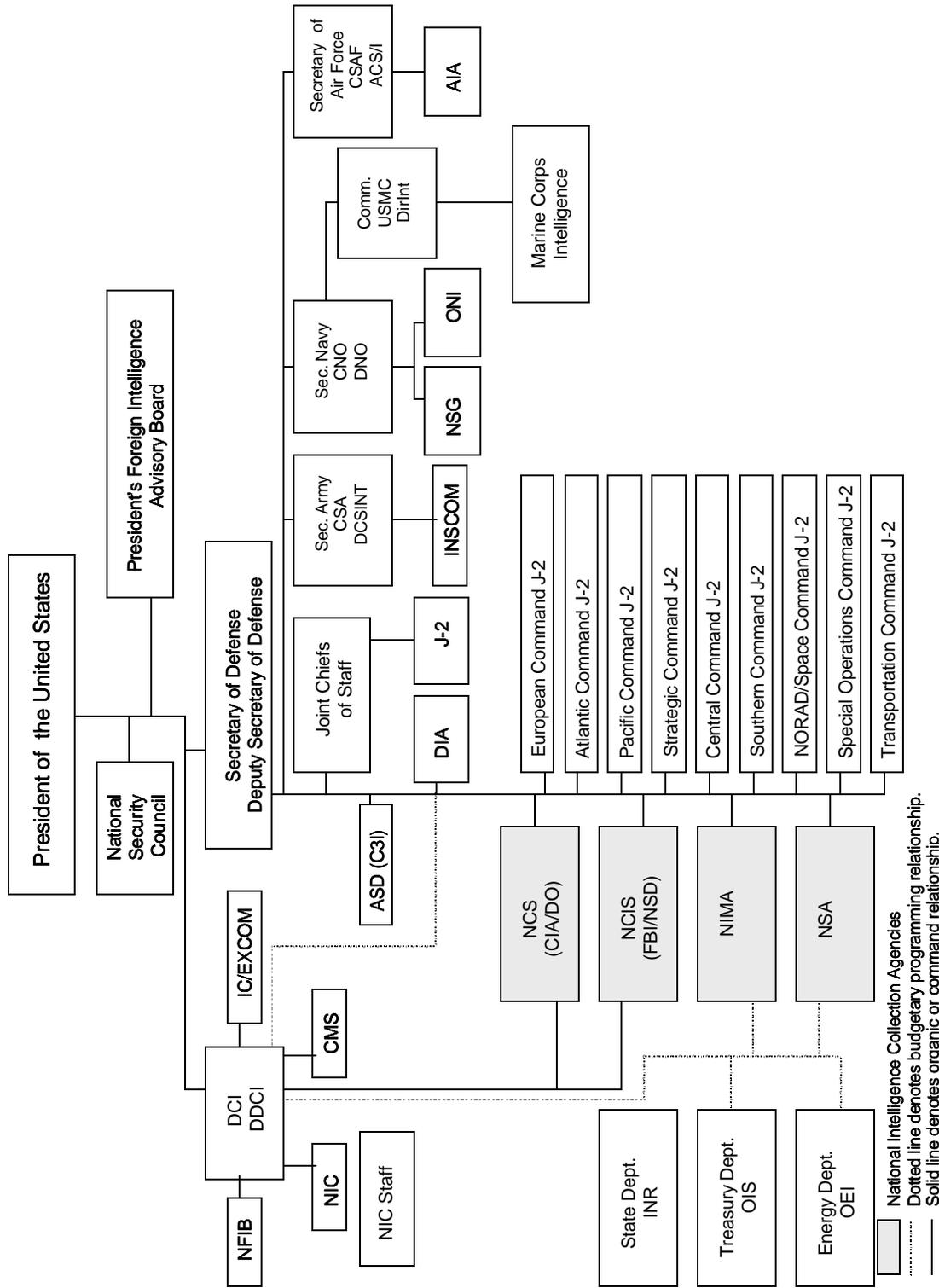


Figure 7. The U.S. Intelligence Community, Showing Proposed Organizational Reforms

Appendix

A Description of the Intelligence Process, and the Organizations Discussed in this Study

This study of the Intelligence Community (IC) focuses on doctrine-based reorganization. In order to follow the report, it is important for the general reader to know the basic functions, elements, and funding mechanisms of the IC. This section accordingly lists and briefly describes the intelligence process, the major IC organizations, agencies, and budgetary components. Further discussion of how they function, and how they work together, is found in relevant chapters. The reader already familiar with the IC need not read this appendix.

The Intelligence Process

Intelligence is a vital element of our national security. There is an absolute need for it and for a U.S. Intelligence Community to provide it. Without intelligence our government and military forces would be at the mercy of better-informed adversaries and competitors.

Intelligence can be defined as knowledge or foreknowledge of relevant aspects of the world around us which is used by U.S. policymakers and military leaders to make decisions [1]. This knowledge is requested by these officials, and so begins the intelligence process or cycle. **Collection management** involves tasking the IC to provide intelligence on certain questions. **Collection** is the gathering of “raw” intelligence or data, which collectors sometimes put into a form that can be used by production offices. In a specialized collection agencies **technical collection management** takes place, where managers orchestrate diverse collection systems on the basis of priority and opportunity. This is a highly complicated and specialized activity that varies greatly among collection agencies, depending on the technologies involved. **Production** divisions of the IC analyze the raw and processed data and produce reports and studies, which can be defined as “finished” intelligence. **Dissemination** is providing the finished intelligence to the consumer, or user. The user then (ideally) provides feedback and additional direction (collection management) to the collectors and producers, who should in turn provide more and better intelligence. This cycle should result in the IC providing timely, useful products allowing informed political and military decisions by U.S. government officials and military officers [2].

The Director of Central Intelligence (DCI)

The Director of Central Intelligence is the statutory head of the Intelligence Community. The DCI is charged with three major tasks: managing the IC at large, directing the Central Intelligence Agency (CIA), and serving as principal intelligence adviser to the President. His office was defined by the National Security Act of 1947. Since 1976, the DCI has been assisted by a Deputy Director of Central Intelligence (DDCI) [3]. In 1996, Congress approved adding a second Deputy Director, for Community Management, and three Assistant Directors of Central Intelligence: One for Collection, one for Analysis and Production, and one for Administration [4]. Several management and coordinating bodies also aid the DCI, and are discussed below.

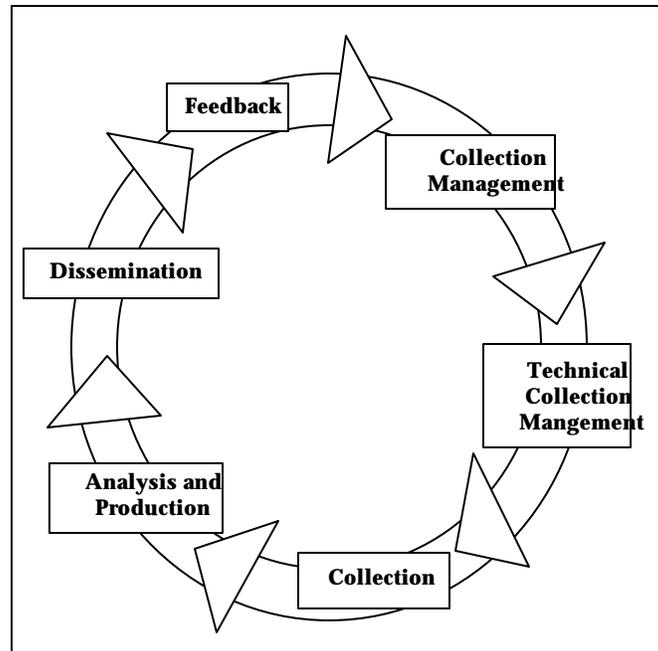
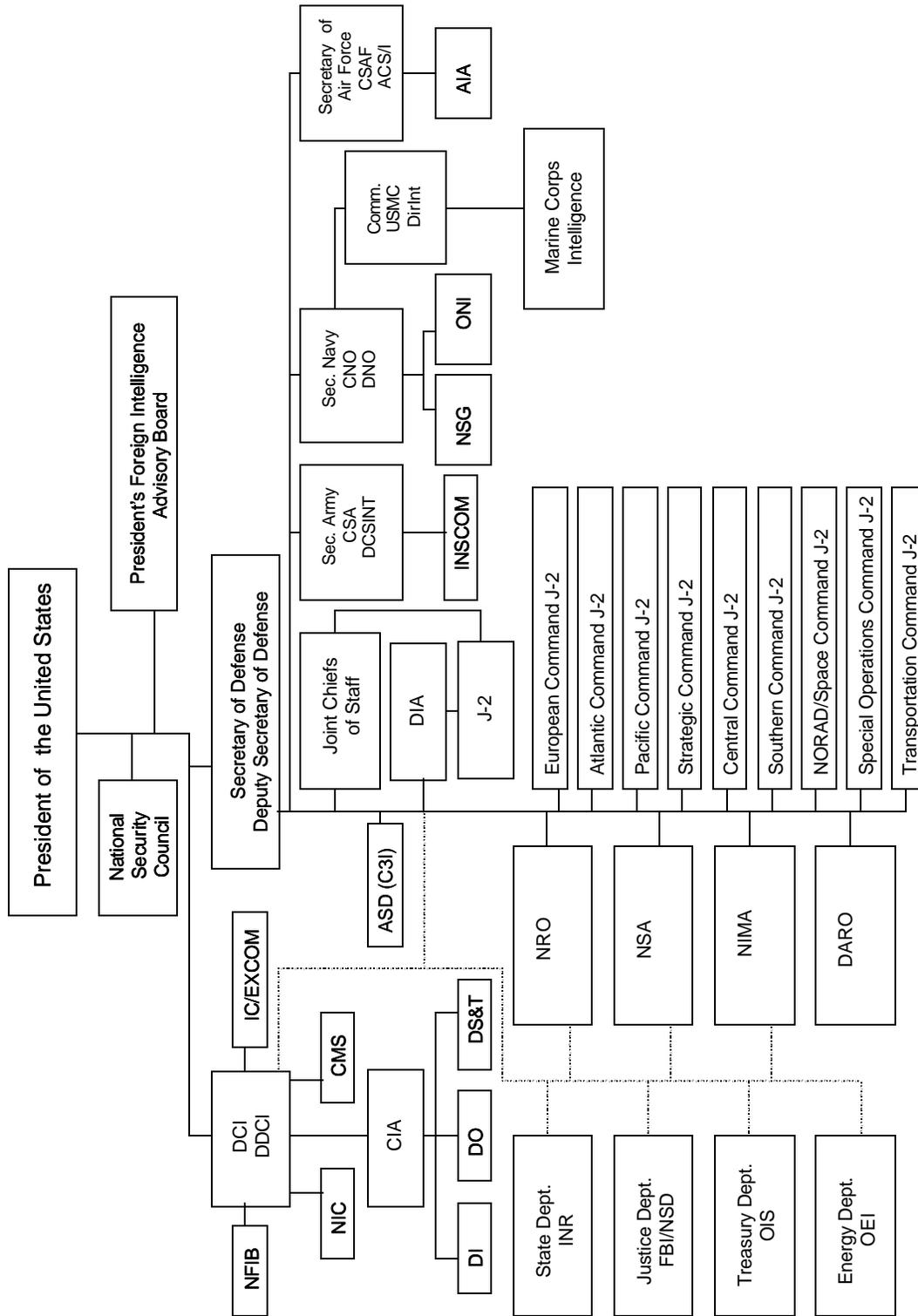


Figure 8. The Intelligence Cycle

The Community Management Staff (CMS)

The DCI in his role as manager of the IC is supported by a Community Management Staff (CMS). The CMS in 1992 superseded the IC Staff (ICS). The CMS develops, evaluates, justifies, and monitors the budget for the National Foreign Intelligence Program (NFIP), which is defined below. The CMS also conducts long-range strategic planning for, and evaluating progress toward, meeting long-range objectives; translating the needs of intelligence consumers into national intelligence needs; integrating the efforts of the collection disciplines, or forms of intelligence, [i.e., signals intelligence (SIGINT), imagery intelligence (IMINT), human intelligence (HUMINT), and measurement and signature intelligence (MASINT)] to satisfy those needs; and evaluating the IC's performance in satisfying those needs. The CMS is headed by the Executive Director for Intelligence Community Affairs (EXDIR/ICA). Currently there are several main offices, referred to as groups, in the CMS: Resource Management; Program Assessment and Evaluation; Requirements and Plans; Policy

and Special Issues; and Advanced Technology. Also resident in the CMS are three IC secretariats: the Quality Council, Intelligence Systems, and Intelligence Program Review Group.



..... Dotted line denotes budgetary programming relationship.

Figure 9. The Current U.S. Intelligence Community

The Intelligence Community Executive Committee (IC/EXCOM)

The Intelligence Community Executive Committee (IC/EXCOM) in 1992 superseded the National Foreign Intelligence Council (NFIC) which was established during the Reagan Administration. The IC/EXCOM aids the DCI with regard to intelligence policy and resource matters; priorities and objectives for the NFIP budget; IC policy and planning; and IC management and evaluation [5]. Membership on the IC/EXCOM is similar to that of the NFIB. The DCI is Chairman and the Deputy DCI is Vice Chairman and CIA representative. Other members include the directors of NSA, DIA, INR, NRO, and NIMA; the Chairman of the National Intelligence Council (NIC); Assistant Secretary of Defense for Command, Control, Communications, and Intelligence; Under Secretary of Defense for Acquisition and Technology; Vice Chairman of the Joint Chiefs of Staff (JCS), and Executive Director for Intelligence Community Affairs [6]. IC/EXCOM meetings are not necessarily limited to principals [7].

The National Intelligence Council (NIC)

The National Intelligence Council (NIC) serves as a senior advisory group to the DCI, and is responsible for determining and promulgating the IC's judgments on issues of importance to policymakers [8]. The NIC is the producer of the National Intelligence Estimates (NIEs) [9]. The NIC includes a chairman; 12 National Intelligence Officers, each of whom covers a major geographical region (e.g., East Asia) or function (e.g., Strategic Programs and Nuclear Proliferation) [10] and a small staff of supporting analysts. Under the NIC is the National Intelligence Production Board, and several other IC-wide intelligence production committees. The NIC was created in 1979; in 1992 it was restructured and moved from its location at the CIA facility in order to underscore its role as an independent, community-wide organization [11].

The National Foreign Intelligence Board (NFIB)

The NFIB is responsible for review and coordination of national foreign intelligence; interagency exchanges of foreign intelligence; arrangements with foreign governments on intelligence matters; and protection of intelligence sources and methods. In practice, most of the board's business has been to review and approve National Intelligence Estimates (NIEs) [12]. NIEs are defined as "the DCI's most authoritative written judgments concerning national security issues. They deal with capabilities, vulnerabilities, and probable courses of action of foreign nations and key developments relevant to the vital interests of the United States" [13].

The NFIB is chaired by the DCI; the board also includes the Deputy DCI as Vice Chairman and CIA representative; the directors of the Defense Intelligence Agency (DIA), the National Security Agency (NSA), and the National Imagery and Mapping Agency (NIMA); the Assistant Secretary of State for Intelligence and Research (INR); the Assistant Director of the Federal Bureau of Investigation (FBI) (Intelligence); the

Special Assistant to the Secretary of the Treasury (National Security); and the Assistant Secretary of Energy for defense programs. The Director of NRO attends as necessary. The senior Army, Navy, Air Force, and Marine Corps intelligence officers sit on the board as observers. NFIB meetings tend to be limited to principals only [14]. The NFIB has existed, under various designations, since the creation of the CIA in 1947; it has used its present name publicly since 1978 [15].

The IC has 13 major organizations that are concerned with producing finished intelligence, gathering raw intelligence, or producing and operating systems that gather raw intelligence. Many of these agencies perform more than one function. They are discussed in turn below.

The Central Intelligence Agency (CIA)

The Central Intelligence Agency was created by the National Security Act of 1947. The Act charged the CIA with (*inter alia*) providing intelligence to the National Security Council, and “perform[ing] other such functions and duties related to intelligence affecting the national security as the National Security Council may from time to time direct.” This broadly written directive provides the justification for the CIA’s HUMINT collection and Covert Action (CA) activities [16].

The CIA includes three major divisions: the Directorate of Intelligence (CIA/DI), the Directorate of Operations (CIA/DO), and the Directorate of

Science and Technology (CIA/DS&T). CIA/DI is the directorate charged with analysis and production of finished intelligence products, based on “all-source” intelligence collection. CIA/DO is charged with the collection of human intelligence (HUMINT) and with conducting covert action. CIA/DS&T operates a number of technical intelligence collection programs, including the Foreign Broadcast Information Service (FBIS), and provides technical support to CIA/DO. In addition, a CIA Directorate of Administration (CIA/DA) provides administrative support to the Agency [17].

The Defense Intelligence Agency (DIA)

The Defense Intelligence Agency (DIA), founded in 1961, is charged with a variety of analytic and collection tasks. Mainly it provides “all source” finished intelligence to DoD for two primary purposes. One purpose is to support the force enhancement process, i.e., to provide threat assessment in order to formulate requirements for U.S. weapon developers, and to improve training and organization. The other main purpose of finished intelligence from DIA is support to military operations. DIA supports the Joint Chiefs of Staff and the Unified Commands in this capacity with an office headed by a two-star military officer, who serves as Director for Intelligence for the Joint Staff (J-2). DIA also administers the Defense Attaché System and the Defense HUMINT Service (DHS), as well as the office that oversees collection of Measurement and Signature Intelligence (MASINT). DIA is headed by a three-star military officer, who reports to the Assistant Secretary of Defense for C3I.

The National Security Agency (NSA)

The National Security Agency (NSA) was founded in 1952. A combat support element of the Department of Defense, it is charged with collecting and disseminating signals intelligence (SIGINT), which it provides to military commands, civilian agencies, and producers of all-source finished intelligence [18]. It is led by a three-star military officer, who reports directly to the Secretary of Defense. NSA's day-to-day operations fall under its Consolidated Cryptographic Program (CCP); NSA also develops SIGINT technology. It is the largest intelligence agency in terms of personnel [19].

The National Imagery and Mapping Agency (NIMA)

NIMA was created on October 1, 1996. It is a combat support element of the Department of Defense. NIMA collects and provides imagery, imagery intelligence, and geospatial (mapping) information (not finished products), in support of national security objectives [20]. NIMA is responsible for the functions of the following disestablished organizations: the Central Imagery Office (CIO), the Defense Mapping Agency (DMA), and the Defense Dissemination Program Office; and performs the functions of the CIA's National Photographic Interpretation Center (NPIC). NIMA also absorbs the imagery exploitation, dissemination, and processing elements of DIA, NRO, and DARO [21]. By statute, NIMA is led by a three-star military officer [22]. NIMA's Director reports directly to the Secretary of Defense.

The National Reconnaissance Office (NRO)

The National Reconnaissance Office (NRO) was established in 1960. An agency of DoD, it is charged with developing, acquiring, launching, and operating space-based reconnaissance systems for the entire IC. The NRO does not produce intelligence itself; its most direct relationships are with the collection agencies in the IC, rather than with intelligence producers or consumers [23]. The director of NRO is also the Assistant Secretary of the Air Force for Space [24].

The Defense Airborne Reconnaissance Office (DARO)

The 1993, the Defense Airborne Reconnaissance Office (DARO) was formed. DARO is a DoD organization charged with management oversight of the development and acquisition of all joint Military Department and Defense-wide airborne reconnaissance capabilities, including manned and unmanned aerial vehicles (UAVs), their sensors, data links, data relays, and ground stations. The hardware programs it manages are integral components of U.S. national IMINT collection capabilities. DARO is led by a 2-star military officer.

Army, Navy, Air Force, and Marine Corps Intelligence

The military services have their own intelligence elements. U.S. Army Intelligence and Security Command (USAINSCOM) is headed by the Deputy Chief of Staff of the Army for Intelligence (DCSINT). Subordinate elements of USAINSCOM collect all-source intelligence information in response to Army, Unified Command, DoD, and national-level collection requirements. The Navy is supported by the Office of Naval Intelligence (ONI), which is headed by a flag-rank Director of Naval Intelligence (DNI). ONI is responsible to the Chief of Naval Operations for intelligence, cryptology, special security, and foreign counterintelligence. Signals security is handled by the Naval Security Group. Marine Corps intelligence is headed by a Director of Intelligence, who is the Senior Intelligence Officer and the Commandant's principal staff officer and functional manager of all-source intelligence, counterintelligence, and cryptologic matters. Air Force intelligence is headed by an Assistant Chief of Staff, Intelligence (ACS/I), who manages Air Force signals, technical, human, and imagery collection efforts [5]. Each service's intelligence is organized somewhat differently. The service intelligence organizations perform a variety of functions, including collection and analysis for force enhancement, and support for military operations [26].

There are nine Unified Commands that have responsibilities for military operations worldwide: European Command, Atlantic Command, Pacific Command, Strategic Command, Central Command, Southern Command, North American Aerospace Defense Command (NORAD)/Space Command, Transportation Command, and Special Operations Command. All have intelligence staff (J-2) sections [27]. Intelligence staffs or officers are also located at all service organizational levels down to battalion in the ground forces, wing or squadron in the air forces, and individual ships in the Navy.

State, Energy, and Treasury Department Intelligence Offices

Besides DoD, several Cabinet agencies have intelligence offices. All are much smaller than CIA or DIA, and serve almost exclusively to provide their agencies with finished intelligence.

The Bureau of Intelligence and Research (INR) produces intelligence for the State Department. It is one of the three intelligence agencies (the others are CIA and DIA) that produce and disseminate “all-source” finished intelligence; INR (unlike CIA and DIA) has no dedicated collection capabilities [28]. The Office of Energy Intelligence is the intelligence arm of the Department of Energy (DoE), and reports on a variety of topics. The Office of Intelligence Support (OIS) is the Treasury's intelligence office, which reports on international financial matters [29].

The Federal Bureau of Investigation (FBI)

The FBI is a law enforcement agency responsible to the Department of Justice. Its sole function within the IC is Counterintelligence (CI). The Assistant Director of the FBI's National Security Division is the senior official responsible for U.S. counterintelligence activities within the United States. Coordination of U.S. counterintelligence activities overseas is the responsibility of the DCI [30], until a matter has become a formal law enforcement investigation, in which case lead responsibility shifts to the FBI.

The Intelligence Budget

The intelligence budget is divided into three major parts. They are the National Foreign Intelligence Program (NFIP), the Joint Military Intelligence Program (JMIP), and Tactical Intelligence and Related Activities (TIARA).

NFIP includes the funding for CIA, and the national foreign intelligence or counterintelligence programs of the State Department, DIA, NSA, NIMA, NRO, the Army, Navy, and Air Force, the FBI, DoE, and Treasury [31]. NFIP is the only part of the intelligence budget that is directly under the purview of the DCI. Most of the NFIP also falls within the defense budget [32]. In Congress, the House and Senate Intelligence Committees have jurisdiction over the NFIP budget, subject to review by the House National Security Committee and Senate Armed Services Committee, respectively.

JMIP comprises defense intelligence elements that support defense-wide, multiple service, or theater-level needs [33]. The JMIP is a budget category introduced in 1994, and mostly consists of programs formerly in TIARA [34]. JMIP is developed by the Defense Department and falls under the responsibility of the Deputy Secretary of Defense [35]. The House Intelligence Committee has jurisdiction over JMIP; but in the Senate, jurisdiction over the JMIP is held by the Senate Armed Services Committee, with the Senate Intelligence Committee staff allowed to participate in staff-level Armed Services meetings and providing for consultation between the chairmen and ranking minority members of the two committees [36].

TIARA are “organic” military intelligence assets and activities that support single-service combatant commands. The TIARA budget is developed by the military services, and as such is an aggregation of service-specific programs. The House Intelligence Committee has jurisdiction over TIARA, but in the Senate, jurisdiction is in the hands of the Senate Armed Services Committee with the Senate Intelligence Committee staff allowed to participate, analogous to the way that JMIP is handled.

Notes

1. See CIA, Public Affairs Staff, *A Consumer's Guide to Intelligence* (Washington: CIA, document number PAS 95-00010, July 1995; hereinafter *Consumer's Guide*), p. vii.
2. *Consumer's Guide*, p. 1.
3. Aspin-Brown Commission, p. 48.
4. Public Law 104-293--October 11, 1996, 110 Stat 3477-3478.

5. *Consumer's Guide*, p. 41; see also *IC21*, p. 74.
6. Aspin-Brown Commission, p. 56n.
7. Mark M. Lowenthal, *U.S. Intelligence: Evolution and Anatomy* (Westport, CT: Praeger, 1992)p. 112.
8. *Consumer's Guide*, p. 15.
9. *Consumer's Guide*, p. 56; Lowenthal, p. 133.
10. *Consumer's Guide*, p. 15.
11. Lowenthal, pp. 132-133.
12. *Consumer's Guide*, pp. 41, 56.
13. *Consumer's Guide*, p. 56.
14. Lowenthal, p. 111.
15. Lowenthal, p. 111.
16. Lowenthal, pp. 18-19; in 1992, Congress amended the National Security Act specifically to authorize the CIA to collect HUMINT, and to provide overall direction of HUMINT collection by other U.S. government agencies. Aspin-Brown Commission, p. 61 n.
17. Aspin-Brown Commission, p. 62.
18. *Consumer's Guide*, p. 23.
19. Aspin-Brown Commission, p. 132.
20. National Imagery and mapping Agency, booklet, "NIMA Establishment Ceremony," (Fairfax, VA: NIMA, 10/29/96) pp. 3, 11.
21. National Imagery and Mapping Agency, Office of Congressional and Public Liaison, media release (fax), 10/1/96.
22. NIMA's first and current head, Rear Admiral J.J. Dantone, USN (a 2-star Admiral), was appointed as acting director.

23. Brig. Gen Robert (Rick) Larned, USAF, Director of Imagery Systems Acquisition and Operations, NRO, briefing slides presented to the Society of Old Crows, Alexandria, VA, 2 October 1996 (fax).
24. *Consumer's Guide*, p. 10.
25. *Consumer's Guide*, pp. 11-12.
26. Aspin-Brown Commission, p. 109.
27. The designation "J-2" for the joint staff ("G-2" or "S-2" in Army staffs) signifies the intelligence function and staff. Staff functions are numbered from 1 to 5. Personnel is 1; Intelligence, 2; Operations, 3; Supply, 4; and Civil Affairs, 5. Each function is served by a staff, the size of which varies depending on the size of the unit.
28. *Consumer's Guide*, pp. 24-27.
29. *Consumer's Guide*, p. 27.
30. Aspin-Brown Commission, p. 58.
31. *C21*, p. 11.
32. *IC21*, pp. 12, 71.
33. *IC21*, pp. 11, 72.
34. Department of Defense Directive, April 7, 1995, Number 5205.9, SUBJECT: Joint Military Intelligence Program (JMIP) (fax). See also Richard A. Best, Jr., *Intelligence Issues and the 104th Congress* (Washington: Congressional Research Service, September 26, 1996, Order Code IB95018), p. CRS-6.

35. See U.S. Congress, Senate, Select Committee on Intelligence (SSCI), *Authorizing Appropriations for Fiscal Year 1997 for the Intelligence Activities of the United States Government and the Central Intelligence Agency and the Central Intelligence Agency Retirement and Disability System and for Other Purposes* (Washington: GPO, Report 104-258), p. 2.

36. SSCI, p. 3.

Biographies

LTG William E. Odom, USA (ret.), served as Director of the National Security Agency from 1985 to 1988. Previously he served as Deputy Assistant and then Assistant Chief of Staff for Intelligence, Department of the Army. From 1977 to 1981, General Odom was military assistant to the President's Assistant for National Security Affairs, Zbigniew Brzezinski. Earlier, as a Russian Area Specialist, he served on the U.S. Military Liaison Mission to Soviet Forces in Germany, and as Assistant Army Attaché in Moscow. His publications include five books and numerous articles. General Odom is currently Director of National Security Studies at the Hudson Institute and an adjunct professor at Yale University.

Lt. Gen. James R. Clapper, USAF (ret.) served as Director of the Defense Intelligence Agency from 1991 to 1995. Previously he served as Chief of Air Force Intelligence, and as Director of Intelligence for three unified military commands: U.S. Forces, Korea; Pacific Command; and Strategic Air Command. General Clapper is currently a Principal with Booz-Allen & Hamilton, Inc.

Dr. William R. Graham served as Science Advisor to President Ronald Reagan from 1986 to 1989, and concurrently as Director of the White House Office of Science and Technology Policy. From 1985 to 1986, he served as Deputy Administrator of the National Aeronautics and Space Agency. From 1982 to 1985, Dr. Graham served as Chairman of the General Advisory Committee on Arms Control and Disarmament. Currently he is President of National Security Research, Inc.

Mr. Robert E. Rich served for forty years in the National Security Agency, retiring in 1990; he served as Deputy Director of NSA from 1982 to 1986. Since retirement, Mr. Rich has participated in a number of studies of government and the intelligence community.

Ms. Elizabeth R. Rindskopf, Esq. served from 1990 to 1995 as General Counsel for the Central Intelligence Agency and senior legal advisor for the U.S. Intelligence Community. From 1989 to 1990 she served as Principal Deputy Legal Adviser, Department of State. From 1984 to 1989, Ms. Rindskopf was General Counsel at the National Security Agency. Currently Ms. Rindskopf is Counsel at Bryan Cave LLP.

LTG Harry E. Soyster, USA (ret.), served as Director of the Defense Intelligence Agency from 1988 to 1991. Previously he served as Deputy Assistant Chief of Staff for Intelligence, Department of the Army, and Commanding General, U.S. Army Intelligence and Security Command. General Soyster is currently Vice President for International Operations at Military Professional Resources, Inc.

Dr. Gregory F. Treverton served as vice-chairman of the National Intelligence Council from 1993 to 1995. Previously he was Senior Fellow at the Council on Foreign Relations, Lecturer in Government at the Kennedy School, Harvard University, and Director of Studies at the International Institute for Strategic Studies, London. From 1977 to 1979, Dr. Treverton served on the National Security Council Staff; from 1975

to 1977, he was a professional staff member on the Senate Select Committee on Intelligence. Dr. Treverton is currently Director of the Center for International Security and Defense Policy at the RAND Corporation.

Mr. Bernard C. Victory is an analyst with the National Institute for Public Policy. He has researched and written on a number of national security topics including missile defense, chemical weapons, long-range strike capabilities, and the congressional impact on defense policy.