IC21: INTELLIGENCE COMMUNITY IN THE 21ST CENTURY

STAFF STUDY

PERMANENT SELECT
COMMITTEE ON INTELLIGENCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTH CONGRESS

DISTRIBUTION STATEMENT A
Approved for public release;
Distribution Unlimited

19960514 010

DTIC QUALITY INSPECTED 1

IC21: INTELLIGENCE COMMUNITY IN THE 21ST CENTURY

STAFF STUDY

PERMANENT SELECT COMMITTEE ON INTELLIGENCE HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTH CONGRESS

U.S. GOVERNMENT PRINTING OFFICE
23-748cc WASHINGTON : 1996

LARRY COMBEST, TEXAS, CHAIRMAN
ROBERT K. DORNAN, CALIFORNIA
C.W. BILL YOUNG, FLORIDA
JAMES V. HANSEN, UTAH
JERRY LEWIS, CALIFORNIA
PORTER J. GOSS, FLORIDA
BUD SHUSTER, PENNSYLVANIA
BILL McCOLLUM, FLORIDA
MICHAEL N. CASTLE, DELAWARE

NORMAN D. DICKS, WASHINGTON
BILL RICHARDSON, NEW MEXICO
JULIAN C. DIXON, CALIFORNIA
ROBERT G. TORRICELLI, NEW JERSEY
RONALD D. COLEMAN, TEXAS
DAVID E. SKAGGS, COLORADO
NANCY PELOSI, CALIFORNIA

NEWT GINGRICH, GEORGIA, EX OFFICIO
RICHARD A. GEPHARDT, MISSOURI, EX OFFICIO

U.S. HOUSE OF REPRESENTATIVES
PERMANENT SELECT COMMITTEE
ON INTELLIGENCE
WASHINGTON, DC 20515–6415

ROOM H–405, U.S. CAPITOL
(202) 225–4121

MARK M. LOWENTHAL, STAFF DIRECTOR
LOUIS H. DUPART, CHIEF COUNSEL
MICHAEL W. SHEEHY, DEMOCRATIC COUNSEL

April 9, 1996

Hon. Newt Gingrich
Speaker of the House
Washington, D.C.

Dear Mr. Speaker:

Staff members of this Committee recently completed a study entitled *IC21: The Intelligence Community in the 21st Century*. This study has been carefully edited in consultation with the appropriate agencies to remove any classified information. The study represents the observations and conclusions of the staff. It does not represent the views of all Members of the Committee.

Sincerely,

Larry Combest

Larry Combest
Chairman

IC21: The Intelligence Community in the 21st Century
Table of Contents

Page

I. Overview and Summary 1

II. Intelligence Community Management 52

III. Intelligence Requirements Process 82

IV. Collection Synergy 96

V. SIGINT: Signals Intelligence 120

VI. IMINT: Imagery Intelligence 122

VII. MASINT: Measurement and Signatures Intelligence 144

VIII. Collection: Launch 174

IX. Clandestine Service 181

X. Intelligence Community "Surge" Capability 223

XI. Intelligence Support to Military Operations 239

XII. Intelligence Centers 256

XIII. Intelligence and Law Enforcement 272

XIV. Intelligence Communications 291

XV. Congressional Oversight 310

XVI. Appendices

A. IC21 Hearings and Witnesses 331

B. IC21 Staff Panels 333

C. CRS Report: Proposals for Intelligence Reorganization 1949-1996 335

Figures:

Figure 1: IC Functional Flow 4
Figure 2: IC21 Staff Studies 6
Figure 3: IC21 Objective Community 49
Figure 4: IC Functions 50
Figure 5: IC Structure and Flow 51

IC21: THE INTELLIGENCE COMMUNITY IN THE 21st CENTURY

Overview and Summary

I. Introduction: What is IC21?

During the 104th Congress, the Permanent Select Committee on Intelligence has undertaken a major review of the role, functions and structure of the Intelligence Community. This review has been called *The Intelligence Community in the 21st Century*, or *IC21*.

This title connotes one of the major premises of the study: that the Intelligence Community (IC) has been largely, and perhaps inevitably, shaped by the Cold War struggle with the Soviet Union. This struggle gave shape to a specific set of "intelligence norms," *i.e.*, organizations, products, practices, relationships and ways of doing business that extend throughout the IC. Some of these intelligence norms are likely to be fairly stable, regardless of U.S. national security policy or the international political environment. Others may be outdated and no longer responsive to U.S. national security requirements as we enter the 21st century. *IC21* seeks to determine which of these intelligence norms are still relevant, which need to be either revised or replaced, and what alternatives there are to be added.

II. Guiding Concepts

IC21 has been guided by the following broad concepts:

- The United States continues to need a strong, highly capable and increasingly flexible IC. This need has not diminished with the end of the Cold War. Indeed, the current international situation is, in many ways, more complex and more difficult to deal with than was the relatively stable bi-polar Cold War. Thus, although we find our national security less threatened, the demands for intelligence remain. The focus of our national security has changed, but the mission of the IC has not changed: providing timely, assessed intelligence to civil and military policy-makers, supporting military operations and carrying out certain operations -- including covert action -- as tasked by legally responsible officials.

- A key issue is *opportunity*, not reform. As noted, U.S. national security interests are less threatened than at any time since 1940. This is a propitious moment in which to review major aspects of our national security apparatus and to update them in an atmosphere relatively free from crises. Although Congress and the Executive continue to deal with issues of the propriety of certain operations, oversight and -- occasionally -- legality, these are not the main driving issues as they were in the mid-1970s.

- Everything is on the table. There are no sacred cows in terms of organizations, missions or functions. Neither are there any preconceptions as to the "right answer" for the future of the IC.

- *IC21* is not an exercise designed to reduce, or even to shape the intelligence budget. The goal is to define the type of IC that will best meet U.S. national security needs into the next century. The question of whether the price for this type of IC is acceptable can only be decided by Congress and the Executive during their budget deliberations.

- *IC21* is not simply an effort to reorganize the IC. Any major recommendation for organizational change must come only from well-defined intelligence or policy-maker needs.

- Although the Committee's purview over the IC is fairly broad, it is important to keep its primary focus on those issues that might require legislative remedies. Changes that can be carried out by or within the Executive should also be noted, as should findings for which no specific recommendations are made.

- Any changes must result in improved processes or products to be worth the cost of short-lived dislocations.

- To the greatest extent possible, the *IC21* process should be public and unclassified. One of the goals of *IC21* is to renew a national consensus to support a strong and capable IC. Such a consensus must rely on an easily accessible body of information. This is an especially important function for, as several witnesses have told the Committee, beyond Congress and the Executive, there is no natural constituency for intelligence in the United States.

- Finally, the focus must be on where the IC needs to be in the next 10-15 years, not a snapshot of where we are today.

III. Methodology

After much preliminary staff study -- aided by a set of detailed questions sent out to over 40 former and current officials with national security experience, academics, and IC veterans -- the Committee undertook *IC21* with the view that it would be most profitable to look at the IC largely in terms of functions across the board, rather than agency-by-agency. It was felt that an agency-by-agency approach would lead to either a confirmation or rejection of the *status quo* without providing a basis for projecting future intelligence needs and how best to meet them. This functional concept has been pursued along a number of parallel paths.

Figure 1 indicates the major IC functions as defined in the *IC21* studies. They are aggregated into three broad groups: management, execution and infrastructure.

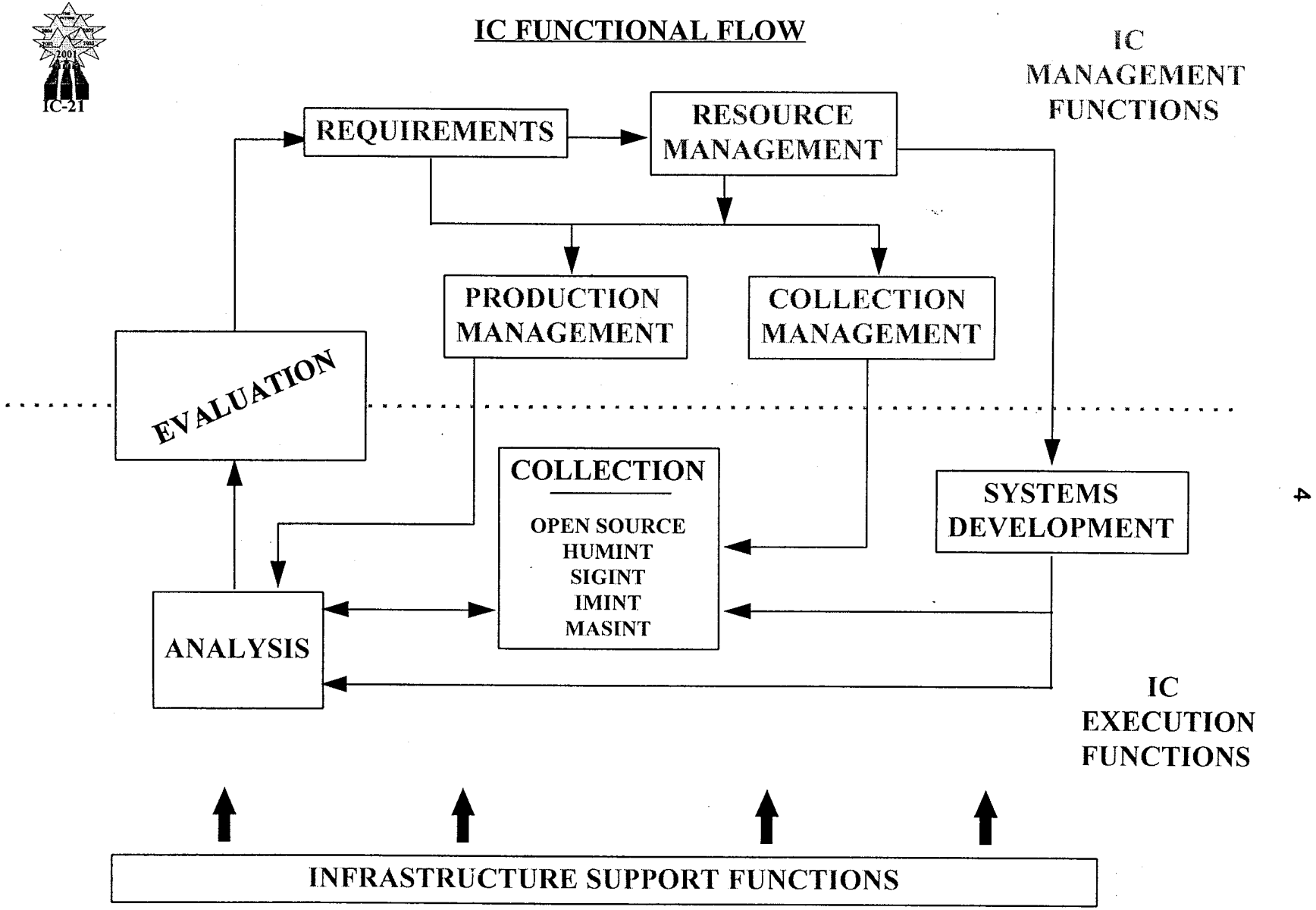

Figure 1: IC Functional Flow

Second, the Committee has held six full committee hearings devoted to *IC21* issues (see Appendix A for a list of hearings and witnesses). All but one of these hearings have been held in open session, in keeping with the envisioned role of *IC21* as a means of building a strong public consensus for intelligence.

Third, Committee staff undertook the 14 studies presented in this volume. As Figure 2 indicates, these studies encompass issues within the broad areas of direction of the IC; intelligence requirements; and collection, analysis and operations. There are no staff studies specifically on intelligence products, although these products clearly would be affected by the recommendations in the staff studies.

IC21 Staff Studies

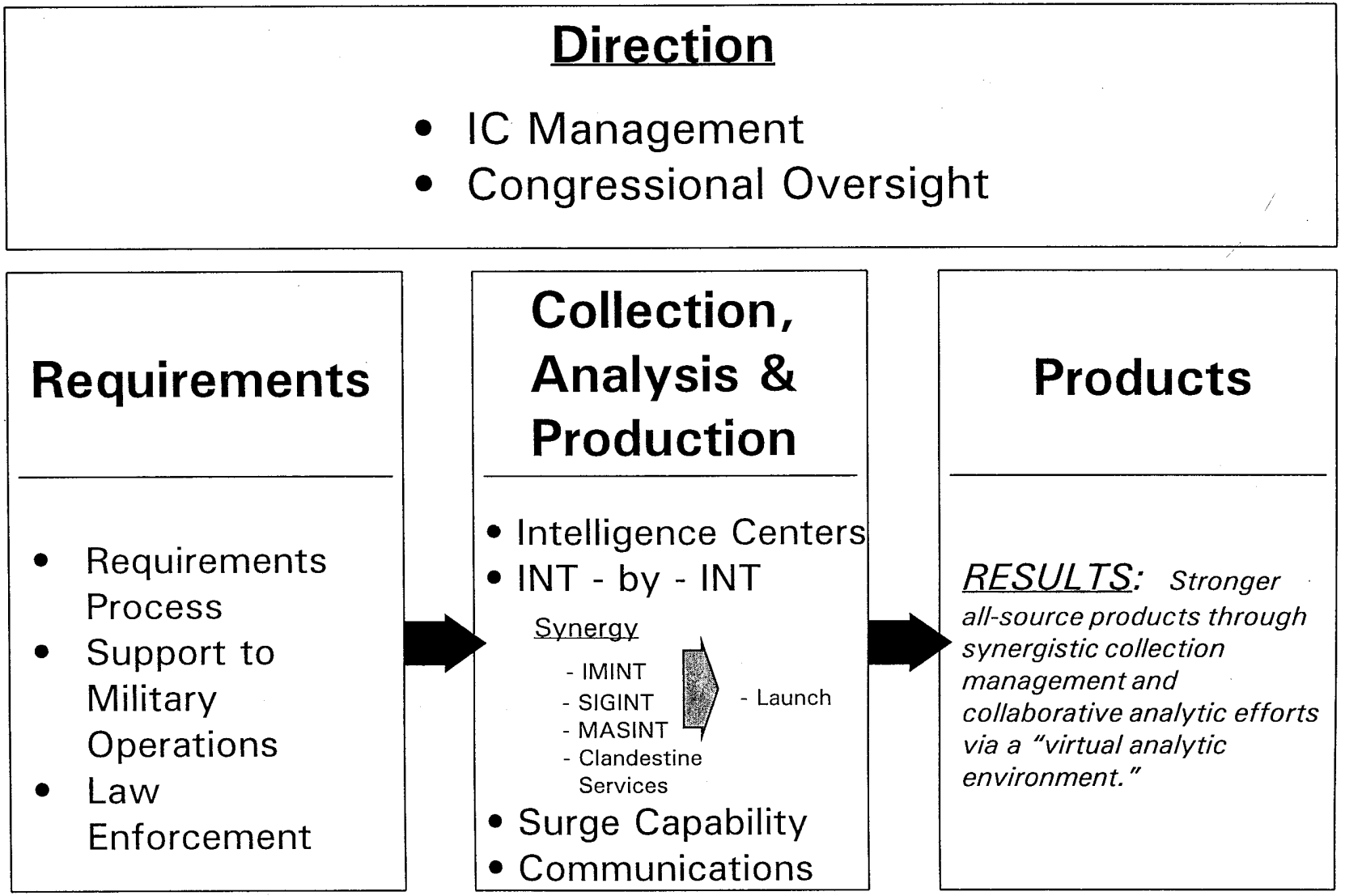

Figure 2: IC21 Staff Studies

Fourth, Committee staff has held 12 formal staff panels with various expert witnesses as part of the background work on the studies. Committee staff also conducted numerous interviews with national security, intelligence and technology specialists in and out of the government on issues specific to the studies. (See Appendix B for a list of staff panels.)

Fifth, the Committee's extensive work on the FY 1996 intelligence budget authorization also yielded a great deal of information relevant to *IC21* issues. This work covered both functional issues and concerns of specific agencies. The Committee held 11 authorization hearings, over 20 Member briefings and more than 200 staff briefings as part of that process.

Finally, the Committee has kept in close touch with other efforts that are re-examining the IC. Chief among these is the commission headed by former Secretary of Defense Harold Brown and, prior to him, the late former Secretary of Defense Les Aspin. Two members of that commission are also Members of the Permanent Select Committee on Intelligence. The staffs of the Committee and the commission have also been in contact throughout the past year. The Senate Select Committee on Intelligence and the Council on Foreign Relations have also been examining some of these same issues. Again, there have been ongoing contact among all of these groups.

IV. Findings and Recommendations: Introduction

At the outset of *IC21* we recognized that we were likely to arrive at a varied set of findings and recommendations, some of which might entail legislation, while others would not. Although our primary focus was and is on areas where Congress can make positive changes and improvements through legislation, we also did not want those other recommendations to be omitted. Therefore, Findings and Recommendations are divided into two groups, the first being those that are being introduced as a bill with a view to action by the Congress, the second being those that we believe the Executive should consider for action on its own.

Overarching Concept: The Need for IC "Corporateness". Throughout the *IC21* process we were struck by the success of the Goldwater-Nichols reforms of the Defense Department in 1986, and we continually referred back to them. Key to the success of Goldwater-Nichols was a central unifying concept: "jointness," the idea that the individual services had to improve cooperation and that a stronger JCS was a major means towards this end.

The IC as we know it today is the result of half a century of *ad hoc* development. Each agency or organization makes sense on its own, but if one were to design an IC today from scratch, this is not likely to be the array that would be chosen. Only intelligence, of all major government functions, is carried out by a very

disparate number of agencies and organizations that are either independent of one another or housed in separate departments headed by officials whose main concerns are policy, not intelligence. Indeed, referring to it as a "community" is more accurate than most people realize, capturing as it does a sense of mutuality and independence.

We believe that the IC has served the nation well, but that given the opportunity we now have to review the functioning of the IC, we can take steps to rationalize some of its functions, to remove some redundancies, to give it greater flexibility and responsiveness to policy maker needs and, above all, to give it a coherence that it has not had.

Indeed, unless one looks at the intelligence process as an integrated whole working towards an agreed end, the IC makes little sense and can become, in its individual parts, self-serving.

We have concluded that a major key to an improved IC is the concept of **"corporateness,"** *i.e.*, for the agencies and employees of the IC to run, to function and to behave as part of a more closely integrated enterprise working towards a highly defined common end: the delivery of timely intelligence to civil and military decision makers at various levels. We believe that this higher sense of corporate identity can be achieved without sacrificing services or functions properly designed to serve more parochial intelligence needs.

- **FINDING: The IC should put greater emphasis on functioning as a true <u>corporate</u> enterprise, in which all components understand that they are part of a larger coherent process aiming at a single goal: the delivery of timely intelligence to policy makers at various levels.**

V. Findings and Recommendations: Legislative Proposal

How the IC is organized and managed is a key set of issues. Ironically, many of the issues in this category studied by *IC21* are among the oldest that have faced the IC, often without any conclusive debate. The longevity of many of these management and structural issues strongly suggests that difficult choices rather than definitive answers are the most likely outcomes as the IC attempts to reshape itself to face new national security issues.

Rather than deal with these issues individually and repeat these old debates, *IC21* gave considerable thought to the broader problems of managing the IC.

The Role of the DCI. Looked at in very simple terms, intelligence consists of three basic tasks: collection, analysis and covert action. But none of these, with the exception of covert action, is carried out exclusively by one agency. Nor does the senior responsible official, the Director of Central Intelligence (DCI), directly control --

either across the IC or even within its non-military portion -- all of those agencies that contribute to these three functions. Ultimately, the components of the IC become internecine competitors. This is most often seen in debates over budgets, but it also becomes apparent in competition among the three functions and within each of them as well.

The role of the DCI is central to this debate. There are two stark choices that would remedy this situation: (1) admit that the concepts of a DCI, of central intelligence and of competitive analysis have not worked and return to a more fractionated intelligence establishment in which components serve their individual policy customers; or (2) attempt to strengthen the central aspects of the IC without losing those facets of individual intelligence service that remain vital. It is the strong conclusion of *IC21* that this second choice, attempting to buttress stronger central features while retaining important independent functions, is the right answer.

- **FINDING: The IC would benefit greatly from a more corporate approach to its basic functions. Central management should be strengthened, core competencies (collection, analysis, operations) should be reinforced and infrastructure should be consolidated wherever possible.**

The role of the DCI is of the utmost importance to achieving this goal. There are two broad areas at stake: (1) the role of the DCI vis-a-vis the President; and (2) the DCI's role within the IC.

Several witnesses, including several past DCIs and Deputy DCIs, noted that the degree to which the DCI visibly commands the respect and confidence of the President is central to the DCI's effectiveness. Realistically, however, there is no way to mandate or to legislate a close working relationship between these two officials. Two suggestions repeatedly surface regarding the status of the DCI. The first is that he be made a cabinet-rank official. The second is that he be given a fixed term of office. *IC21* does not believe that either of these has sufficient merit or would achieve the goal of a stronger DCI. A third suggestion is that he be relieved of his responsibilities for the Central Intelligence Agency (CIA) and elevated to a position over the entire IC.

Cabinet-rank for officials who are not members of the Cabinet (*i.e.*, the heads of departments) is merely an honorific. The United States does not have Cabinet government; being designated a member of the Cabinet does not in any real sense increase one's authority. It certainly will not enhance or improve the DCI's relationship with the President, which can only be based on a level of trust and confidence. Indeed, mandating Cabinet-rank for the DCI while doing anything less than creating a true Intelligence Department -- which no one has contemplated -- only calls more attention to the disparity between the DCI's responsibilities and his authority, even with the enhancements being proposed here.

The importance of the DCI's personal relationship with the President is also the main argument against a fixed term. Proponents of a fixed term argue that this would have several benefits. Ten years is often suggested, as has been done with the Director of the Federal Bureau of Investigation (FBI). First, and perhaps foremost, a fixed term would provide for greater continuity and stability than we now have. Until 1977, it was not customary for the DCI to be replaced with a new administration. That is no longer the case. Moreover, the DCI's position has since been subjected to fairly frequent turn-overs over and above presidential transitions. From 1973-1977 there were five DCIs; from 1991-1996 there have been four DCIs. However, a fixed term could create the situation where a President would inherit a DCI with whom he could not work. Although there would be greater continuity, the DCI's effectiveness would diminish rapidly, a far greater loss. As noted, an analogy is often drawn to the Director of the FBI. The comparison is inapt. First, the ten year term for the FBI Director was enacted to *limit* tenure, not to ensure continuity from one administration to the next. Second, the DCI is the chief intelligence officer and deals directly with the President. The Director of the FBI is not the chief law enforcement officer; the Attorney General is and serves at the President's pleasure. In sum, a fixed term would not be an improvement.

The National Security Act states that the DCI is the head of the IC and the President's principal intelligence adviser. Neither of these designations for the DCI is the same as meaningful control. If the IC is to achieve a greater degree of centrality and corporate identity, then the role of the DCI has to be changed. The glaring gap between his responsibilities and his authorities has to be closed to the greatest extent possible. The DCI should be viewed as a chief executive officer (CEO) of the IC, with purview over all of its major functions and a greater degree of control over budgets, resources and major policy issues that are common to all agencies. To do this in a more coherent and more meaningful manner, the DCI needs managerial resources dedicated to the operations of the entire IC -- a strengthened Community Management Staff (CMS) -- and more authorities than are available to him today.

- **FINDING: The DCI requires additional authorities in order to manage the IC as a corporate entity. Further, the DCI can only be effective in his job if he has a close working relationship with the President and a strong bureaucratic base of his own. "Cabinet status" for the DCI is largely irrelevant and actually may be harmful.**

As noted, we do not find major flaws in the broader parameters of the role of the DCI as currently described in legislation in terms of his tenure or his responsibility for the CIA. Indeed, the testimony of former DCIs and other former senior IC officials all concur that the DCI needs an agency "of his own" -- *i.e.*, the CIA -- if he is to have any real power within the IC. Therefore, we would expand and strengthen the DCI's authorities to include organizational changes that follow.

- **RECOMMENDATION: The DCI should continue to serve at the pleasure of the President, shall exercise direct control over the Clandestine Service, and continue to exercise control over the CIA and the CMS via his deputies.**

If the IC is going to achieve the goal of "corporateness," and if the DCI is going to function as a true CEO, then he should have a greater say in the selection of his "corporate team" -- the heads of the other major intelligence components. Current law requires that the Secretary of Defense "consult" with the DCI in naming heads for National Foreign Intelligence Program (NFIP) defense agencies. Although it is unlikely that the Secretary of Defense would nominate someone to whom the DCI is strongly opposed, it is possible. Instead, the DCI's *concurrence* should be sought. In the unlikely event of disagreement, the issue could be referred to the National Security Council (NSC) Committee on Foreign Intelligence (see below) or, ultimately, to the President. But the importance of a truly corporate team requires a stronger DCI voice in this process.

A similar case could be made regarding the selection of the heads of the departmental intelligence units in the Departments of State, Energy and Treasury. We concentrated only on the Defense NFIP agencies because of the larger importance and role of these entities within the IC, especially in the area of collection, which cannot be claimed by these non-Defense intelligence offices. This aspect of the relationship between the IC and Defense, as well as the changing, more dynamic use of intelligence in military operations, warrant this step.

- **RECOMMENDATION: In order to create a corporate intelligence team, the DCI should have a stronger voice in the appointment of directors of NFIP Defense agencies. The Secretary of Defense should obtain the *concurrence* of the DCI in these appointments.**

It is a Washington truism that the power to shape and control budgets is the essential bureaucratic lever for any manager. The IC budget is currently divided into three major parts:

- NFIP: The National Foreign Intelligence Program, comprised of the entire CIA budget and the national foreign intelligence or counterintelligence programs of the Defense Department; Defense Intelligence Agency (DIA); National Security Agency (NSA); the Central Imagery Office (CIO); the National Reconnaissance Office (NRO); the Departments of the Army, Navy and Air Force; the Departments of State, Treasury and Energy; the FBI; and Drug Enforcement Agency (DEA).

- JMIP: The Joint Military Intelligence Program, comprised of defense intelligence elements that support defense-wide or theater-level needs.

- TIARA: The Tactical Intelligence and Related Activities, comprised of the array of reconnaissance and target acquisition programs that are a functional part of the basic military force structure and provide direct information support to military operations.

This organization may make the overall IC budget more manageable, but it also has the effect of atomizing it into areas that are treated as distinct and separate entities, rather than as parts of a larger whole. This arrangement makes it very difficult to oversee intelligence as an end-to-end process or as a corporate entity.

- **FINDING: IC management has been unable to look at activities, budgets and programs on an IC-wide basis. Instead, these have been looked at as three distinct blocks: NFIP, JMIP and TIARA.**

Although the DCI has IC-wide responsibilities, only the NFIP comes directly under his purview. Within the NFIP budget, however, the individual program managers, i.e., those people who are responsible for developing and overseeing the various NFIP programs, have a great deal of power, so much so that the NFIP is more an aggregation of a variety of types of activities (some agencies, some collection disciplines, some management activities, etc.) rather than a coherent whole.

- **FINDING: The DCI lacks the requisite authorities over the NFIP program managers so that he can manage the IC as a corporate entity.**

The DCI's ability to control the NFIP budget is also complicated by the fact that a substantial number of organizations included in the NFIP are part of the Defense Department. Thus, it is crucial that the DCI be able to work closely with the Secretary of Defense, whose day-to-day control over intelligence dollars and personnel actually exceeds that of the DCI.

- **FINDING: The vast majority of the NFIP budget is within the Defense budget. The DCI should have increased programmatic control commensurate with his intelligence responsibilities, but can only do so with the cooperation of the Secretary of Defense.**

If the DCI is going to manage the IC on a more corporate basis, then he needs greater authority over the program managers. Similarly, only the DCI has the IC-wide oversight and responsibility to look at the budget as a whole, over and beyond these separate programs. He should have the authority to transfer limited amounts of money between NFIP programs or agencies without the programs manager's approval. Inevitably, there will be a need to appeal such decisions. This can either be done directly with the Secretary of Defense or, if necessary, within the NSC Committee on Foreign Intelligence (see below).

- **RECOMMENDATION: Section 104(d) of the National Security Act should be changed so that the DCI can transfer limited amounts of money between NFIP programs or agencies without the program manager's approval.**

People are the key element of the IC. All of the collection capabilities are machines unless there are dedicated people behind them -- building them, operating them, processing the data, analyzing it. In the area of personnel management we find, again, that there are gaps between the DCI's responsibility and his current authority. At present, only the personnel at CIA are under his control. If he sees an intelligence need that can best be filled elsewhere, he can ask for those people, but he cannot be assured of getting them. In an era in which much greater emphasis is being put on multi-disciplinary analysis and on the use of IC centers (see below), this lack of authority becomes debilitating. The DCI should have authority over all NFIP agency personnel, including the right to assign them where they are most needed.

- **RECOMMENDATION: Expand the authority of the DCI over personnel in all NFIP agencies. This should include the ability to detail personnel from one agency to another, as needed, to best meet IC and policy maker requirements. It should also expand the DCI's termination authority to all NFIP agencies.**

NSC Supervision: Committee on Foreign Intelligence. As noted, the National Security Act designates the DCI as the President's principal adviser on intelligence. This act also places the DCI under direction of the NSC. The NSC is composed of four officials: the President, the Vice President, and the Secretaries of State and Defense. The IC is a service organization. It has no meaning without its relationship to policy makers. Thus, the DCI must have regular contact with the NSC members. However, it is not reasonable to expect that they can give the DCI and, through him, the IC, the kind of regular executive guidance that was envisioned by the National Security Act. Indeed, in each successive Administration, there has been some sort of sub-NSC group created to deal with intelligence, reflecting the shortcomings of the NSC itself to carry out this role.

- **FINDING: Although the DCI should remain under the statutory direction of the NSC, that body itself is rarely capable of providing the consistent high-level guidance that is required.**

Of the various sub-NSC bodies that have been created to deal with intelligence, the Committee on Foreign Intelligence (CFI) created by President Ford in 1976 appeared to be among the more successful, in terms of its stated role, its membership and its performance. Interestingly, the Senate Select Committee on Intelligence proposed re-establishing this group in legislation in 1992, as has the Aspin-Brown Commission. We believe that the CFI, properly constituted and empowered, can more

usefully serve as a body to provide the DCI and the IC with the necessary guidance and policy-maker oversight. This is not meant to supplant the DCI's current direct access to the NSC members; it is meant to give the DCI access on a more regular basis to senior policy-makers who can give direction to the IC and can listen to and relay IC concerns.

- **RECOMMENDATION: The DCI is the principal adviser to the President for intelligence matters, and operates under the direction of the NSC.**

- **RECOMMENDATION: Within the NSC, reestablish a Committee on Foreign Intelligence (CFI) to provide more regular policy guidance, feedback and executive oversight to the DCI.**

- **RECOMMENDATION: The CFI would be comprised of the Assistant to the President for National Security Affairs, who should be the CFI chairman; the Secretaries of State and Defense; the Chairman of the JCS; the DCI; and the Attorney General, or their deputies.**

Deputy Directors of Central Intelligence. We envision that the DCI would continue to have two major responsibilities: for the IC and, within it, for the components that today constitute the CIA. All DCIs have found this a broad and sometimes difficult mandate. Each DCI has shown a preference for one aspect of his job or the other. The ability to delegate is important, although it has been done differently by virtually each DCI. The current DCI, for example, relies on two executive directors -- one for the CIA and one for the CMS. Their titles belie their responsibilities. The positions responsible for these two large parts of the DCI's portfolio should be enhanced and their duties better defined. Some permanence in the DCI's supporting structure is needed and can be achieved without losing necessary flexibility. It also allows for greater institutional continuity, clearer definition of responsibilities and improved congressional oversight.

In order to minimize superfluous bureaucratic layering, one Deputy DCI (DDCI) should specifically be given day-to-day responsibility for the CIA, whose enhanced analytical responsibilities are discussed below. This would reduce layering, would continue to give the DCI direct access to his major bureaucratic and institutional base, and yet would relieve the DCI of many lesser administrative concerns. In addition, there should be a second DDCI for Community Management, for much the same reasons, with purview over the collection, acquisition and infrastructure elements of the IC.

As noted above, the importance of the DCI's relationship with the President is such that few prerequisites for nominees should be imposed. However, to the extent possible, these DDCI positions should be considered as professional as well as political appointments and should go to individuals with extensive national security or

intelligence background. This is especially important if a DCI with less such background is chosen. Given the important of these positions, the two DDCIs should be confirmed by the Senate, just as is the current DDCI position.

- **RECOMMENDATION: Create an additional DDCI position.**

- **RECOMMENDATION: One DDCI will direct the CIA and, to promote corporateness, be responsible for managing <u>all</u> IC analysis and production.**

- **RECOMMENDATION: To further promote corporateness, a DDCI for community management (DDCI/CM) will**

  -- oversee the CMS and

  -- be responsible for IC-wide budgeting, requirements and collection management and tasking, consolidated infrastructure management (in the new Infrastructure Support Office -- see below) and system acquisition.

- **RECOMMENDATION: The DCI will designate one of DDCIs to serve as the Acting DCI in his absence.**

The National Security Act currently mandates that either the DCI or the DDCI can be an active duty military officer, but at no time can both be active duty military officers. We believe this is a sound provision, and would extend it to include the additional DDCI as well.

- **RECOMMENDATION: Both DDCIs should have extensive national security experience; both will be confirmed by the Senate. At no time may more than one of these three (DCI, two DDCIs) be an active duty military officer.**

The growth and development of the IC into distinct agencies has led to unwarranted duplication in what are, essentially, administrative and logistical functions. This is not only duplicative and costly, but also can harm the ability of the IC to operate as a corporate whole. There is no reason why many of these services cannot be merged and run by a single entity -- a new Infrastructure Support Office (ISO).

- **RECOMMENDATION: Consolidate and rationalize management of infrastructure and services of common concern across the IC. These should include at least personnel management, community-level training, security, information systems and communications, managed by the ISO, reporting to the DDCI/CM.**

Director of Military Intelligence. The Defense Department -- civilian policy makers and military services at all levels -- is one of the largest components and most important customers of the IC. Many of the larger organizational issues noted for the IC at large are also found within the defense-related part of the IC. Enhancing the DCI's authority solves some, but not all, of the problems. It is important that the defense intelligence establishment also have a single official who is both responsible for and empowered to address these issues. We believe that this should be a uniformed officer, carrying the title of Director of Military Intelligence (DMI).

- **FINDING: In addition to a strengthened DCI, there should be a DMI with increased authority over non-NFIP defense intelligence programs and direct access to the Secretary of Defense.**

Like the DCI, the DMI also requires a bureaucratic and institutional base, in this case the DIA.

- **RECOMMENDATION: The Director of DIA is to be formally designated as Director of Military Intelligence, the Secretary of Defense's senior uniformed military intelligence officer.**

Some have raised the concern that such a designation, while buttressing defense intelligence, could over-empower the DMI, making him a difficult rival to the DCI. We do not believe that this is likely, given the broader authority of the DCI for all IC-wide activities.

- **RECOMMENDATION: The DMI is a senior member of the U.S. Intelligence Community and will be accountable to the DCI in all matters relative to the IC.**

Clearer responsibility should also be given for JMIP and TIARA. Given that these are not national programs, but are focused more exclusively on military needs, the most logical candidate for this would be the DMI. The DMI should not only be responsible for the JMIP budget, but should also oversee how TIARA is connected to and interacts with NFIP and JMIP.

- **FINDING: The NFIP, JMIP and TIARA budgets should be retained but rationalized. The DMI should be responsible for building the JMIP and overseeing how TIARA connects to and interacts with NFIP and JMIP.**

The DMI's authority over budgets is crucial to his success. The DMI should have broad authority over the two major parts of the defense intelligence budget, the Joint Military Intelligence Program (JMIP) and the Tactical and Intelligence-Related Activities (TIARA). The DMI, through his DMI staff, which works closely with the

CMS, ensures that JMIP and TIARA are coordinated with the NFIP in looking at an overall IC budget.

- **RECOMMENDATION: The DMI will be the program manager of the JMIP and program coordinator for TIARA.**

Community All-Source Analysis. The ability to collect a variety of information on issues or questions from multiple sources is one of the major strengths of the U.S. IC. It gives breadth and greater credibility to analysis. "All-source" analysis, properly done, is of tremendous service to decision-makers.

The CIA, which would now be directed by the DDCI, was envisioned by President Truman as a coordinator of disparate intelligence being produced by other agencies. The CIA quickly became a producer in its own right because of policy-maker demands, the unwillingness of then-existent agencies to respond, and an aggressive CIA leadership. Although this is different than President Truman's vision, we do not believe that this development should be reversed. Indeed, it would appear more profitable to underscore the CIA's analytical role by confirming it as the premier all-source (*i.e.*, deriving its analysis from all intelligence collection disciplines) analytical agency within the IC. No other agency -- DIA, State's Bureau of Intelligence and Research (INR) -- can credibly make that claim.

- **RECOMMENDATION: The CIA's role as the premier all-source analytical agency should be reinforced and underscored.**

We concur with the observation of former DCI Richard Helms that the President needs his own analytical group and that if we did not have the CIA today we would probably invent it. Underscoring this role means more than words. The CIA should include not only its analysts, but a significant number of second- and third-tier exploiters of the various intelligence collection disciplines. By bringing them closer together we can achieve a true synergy between collection and analytical production, rather than keeping them separate to the point where they sometimes seem like competitors rather than parts of a larger corporate process.

- **RECOMMENDATION: To do so, the CIA should house not only analysts, but also second- and third-tier exploiters of the various collection disciplines, in order to create a true synergy between collection and production.**

Confirming this role for the CIA is not meant to diminish the importance of DIA to its Defense customers. DIA consistently plays three key roles in the Defense intelligence process: as an all-source analytical and production capability providing products tailored to Defense officials' needs and in support of military operations; as part of the larger IC competitive analyses; and management of Defense intelligence

production so as to reduce unnecessary duplication. DIA's significant all-source role argues strongly that it, like CIA, should include second- and third-tier exploiters of the various collection disciplines.

- **RECOMMENDATION: The DIA's role as the focal point for management of Defense all-source analysis and production should be reinforced. (No legislative change.) DIA should also house second- and third-tier exploiters of the various collection disciplines.**

Nor should this role for the CIA diminish the role played by other departmental intelligence entities for their specific consumers. They are also necessary to the concept of competitive analysis, which we believe is useful to decision-makers throughout the government. Moreover, each of these offices also contributes to IC-wide analyses, such as National Intelligence Estimates.

- **RECOMMENDATION: State/INR, Energy's Intelligence Office and the Treasury's Intelligence Office should continue to be the primary analytical producers for their departmental consumers. (No legislative change.)**

Community Collection. Many people, when they think about intelligence, think about spies or perhaps satellites -- collection. Collection by a variety of secret methods is, in large measure, what sets the IC apart from other information sources -- either within the government or in the private sector.

A. Clandestine Service. Clandestine activities are what most people think about when they hear the word "intelligence:" Human Intelligence (HUMINT) collectors (spies) and people carrying out covert action. These capabilities are housed primarily, but not exclusively, in the CIA's Directorate of Operations (DO). This aspect of the IC remains the most controversial, the most charged politically, and frequently a major area of contention in congressional oversight.

We did not, as part of *IC21*, take up the issue of the propriety of these activities. There will be a continuing need for HUMINT, as a major means of getting access to plans and intentions. Similarly, we cannot see any reason to forswear the ability to undertake covert actions completely. This capability remains necessary and -- when used properly within the context of well-defined policy and operational goals, executed by legally responsible officials and with due executive and congressional oversight -- it remains important.

- **FINDING: The U.S. will continue to need the capabilities to collect HUMINT, especially as a major insight into intentions and plans of hostile states or groups, and to carry out covert action.**

These are difficult tasks and should only be undertaken by individuals who not only have the unique abilities required, but who adhere to the highest professional standards and all legal requirements.

- **FINDING: The U.S. requires a Clandestine Service of the highest professional standards and competence.**

Clandestine collection entails many more risks than the technical collection disciplines. Therefore, how and when it is used must be highly selective, responding to carefully screened and highest priority requirements.

- **FINDING: Clandestine collection must be focused principally on select, high priority national and military requirements.**

Clandestine collection is also a difficult capability to use. It cannot be kept "on the shelf" and called out whenever needed. There must be some minimal ongoing capability that can be expanded in response to consumer needs. This has become increasingly difficult for the DO as the State Department, in response to budget stringencies, has scaled back its posts overseas, which provide the main base for clandestine collection. Former DCI Woolsey noted that U.S. intelligence was going from "global presence" to "global reach." This scaled back status makes it much more difficult for clandestine services to respond to unanticipated collection requirements.

- **FINDING: It is necessary to have at least a minimal clandestine presence in most countries (a "global presence") so as to maintain a broader base-line contingency capability and to respond to transnational collection requirements.**

Having accepted the necessity for maintaining and, on occasion, using covert action, we also recognize that these operations require the most careful management, expertise and coordination. As one witness at an *IC21* staff panel observed, these are the operations that inevitably land the DCI in trouble. This tendency can be minimized if careful attention is paid to the command and control of clandestine operations.

- **FINDING: Clandestine operations require an extraordinarily high level of management attention, expertise and coordination.**

Under the current arrangement, the Deputy Director for Operations (DDO) is three layers removed from the DCI, having between them the Executive Director of the CIA and the DDCI. Even though the DDO can, presumably, see the DCI whenever necessary, this distancing is too great.

The observation about the DO being the place that most often lands the DCI in trouble rings very true. It should be made into a separate service and brought under the DCI's direct control. This single Clandestine Service (CS) should include those components of the Defense HUMINT Service (DHS) that undertake clandestine collection as well. We do not believe that this division is of utility in terms of collection. We are especially concerned that the Defense Department is unlikely to give DHS the kind of authorities, attention, resources and career development incentives that it will need to become a truly capable clandestine human collection enterprise. Just as intelligence struggled for years to be recognized as a career speciality within the armed forces, DHS faces the same challenge.

- **FINDING: The Defense Department is unlikely to give DHS the kind of attention, resources and career development incentives that it will need to become a truly capable clandestine human collection enterprise.**

We believe that these two entities should be consolidated into one CS under the operational control of the DCI. This is not meant to preclude the Service Intelligence Chiefs from carrying out those clandestine collection activities specifically related to the tactical needs of their Military Departmental customers or field commanders.

- **RECOMMENDATION: The Clandestine Service will be responsible for all clandestine human collection (current CIA/DO and DHS) and shall be under the direct control of the DCI.**

The unique activities of the CS are such that it cannot be managed within the IC as simply another collection discipline. It is the only arm of the U.S. government that has as a principal mission the breaking of foreign laws, something it does on a daily basis around the world in the face of concerted counterintelligence efforts by hostile foreign governments. Managing the CS is markedly different that managing satellite-borne reconnaissance systems or listening posts on U.S. soil.

Moreover, the CS is more than an intelligence collection entity. As several former DCIs have pointed out, the clandestine services are also the DCI's most important "action arm," not only running covert action programs at the direction of the President (a function whose utility we believe will continue to be important), but also in managing most the IC's liaison with foreign government leaders and security services. Each former DCI agreed that these activities demand the DCI's close executive control. Finally, history has shown that the DCI cannot avoid responsibility for being informed about and overseeing the activities of clandestine services. Accordingly, he must avoid any management structure that attenuates his command and control of the CS.

- **FINDING: The mission and management of the Clandestine Service are unique and demand direct accountability to, and control by, the DCI.**

Given the political and administrative problems raised by clandestine operations and covert action, their bureaucratic tie to the DCI must be made more direct. At present as many as two or three officials are between the DCI and the CIA's DO. Moreover, there are no compelling substantive reasons for the DO to be part of the same agency as the analytic Directorate of Intelligence (DI). This is largely the product of historical accident and the bureaucratic aggressiveness of DCI Walter Bedell Smith, who expanded CIA activities into both operations and analysis in the early 1950s, when other agencies failed to meet policy-maker needs in these areas. Indeed, there is a certain "apples and oranges" aspect to attempting to manage both of these functions within one agency.

- **FINDING: The current arrangement of housing analysis and operations in one agency is the result of historical accident rather than well-thought needs. It complicates the management of both activities.**

We believe that having the CS as a distinct entity, under the direct control of the DCI, would rationalize the structure of the CIA as the premier all-source analytical agency and reinforce the unique and highly valuable contributions of clandestine operators. The CS and the CIA can continue to be housed in the same building. However, both the CS and the CIA could also be managed more effectively if they each had one major task.

- **RECOMMENDATION: The Clandestine Service is to be separate from CIA, reporting directly to the DCI.**

Clandestine collection and covert action is not a place for amateurs. The CS should be managed by a director chosen by the DCI from among the ranks of career intelligence professionals. However, this is not meant to limit the choice only to those who have served in the CS. In a more corporate IC, there will be senior managers who are not career CS employees but whose managerial skills and breadth of experience may make them suitable candidates to be the Director of the CS. After much debate, we recommend that this individual not be subject to confirmation by the Senate. The sensitivity of this position is such that the DCI must be free to choose the man or woman upon whom the utmost reliance can be placed. Senate confirmation raises a number of other political considerations that might best be avoided.

- **RECOMMENDATION: The Director of Clandestine Services is to be selected by the DCI from among intelligence professionals.**

We recognize that the CS undertakes some activities specifically designed to support military operations. Indeed, there has been a growing emphasis on this since the Gulf War. This is an important activity and should not be curtailed. Nor is that

the implication of the creation of a single CS, including elements of DHS. In order to assure that there is someone within the CS who is responsible for and extremely knowledgeable about such operations, there should be a Deputy Director of two-star rank for these activities.

- **RECOMMENDATION: There will be a Deputy Director of the Clandestine Service, who is a two-star professional military intelligence officer, responsible for coordination between the Clandestine Service and the various military and Defense components.**

The CS should continue to be seen, however, as an IC asset. HUMINT is and should be part of a larger IC-wide collection plan. Thus, the CS should be responsive to and tasked by the IC-wide collection management process under the DDCI/CM.

- **RECOMMENDATION: For intelligence collection tasking and requirements purposes, the Clandestine Service should respond to the IC-wide collection management process.**

Under current arrangements, the DO receives necessary technical support from offices within the CIA's Directorate of Science and Technology (DS&T). These offices should be made organic to the CS, as should its administrative support offices. The remaining DS&T offices would come under the new Technology Development Office or new Technical Collection Agency, both of which are discussed below.

- **RECOMMENDATION: The Clandestine Service should have organic administrative and technical support mechanisms that are critical to its unique functions and essential to its success.**

B. Technical Collection Agency. The most common criticism of the current collection management process, and one in which we concur, is that it is dominated by "stovepipes," *i.e.*, types of collection that are managed so as to be largely distinct from one another. There are several net results. First, the collection disciplines become competitors for resources driven as much by bureaucratic imperatives as by a broader national need. Second, it also becomes much more difficult to make educated IC-wide decisions about overall collection needs and the resources required to implement them. Breaking down the "stovepipes" was one of the more frequently heard suggestions during the *IC21* process. Remarkably, the current trend within the IC seems to be one that would reinforce the stovepipe approach, further compounding problems for little or no perceived gain.

- **FINDING: The collection management process at the IC-wide level does not routinely integrate the discipline stovepipes.**

The stovepipe system also has a direct effect on analysis. Ideally, there should be some sort of synergy among the various types of collection. A HUMINT report should lead to an image as a means of confirmation; an intercepted signal should confirm a HUMINT report, etc. Instead, there are added difficulties in terms of analysts being able to use all types of intelligence on a routine basis. A system that should be highly synergistic is, instead, fragmented and internally competitive. This will become increasingly important as the complexity of national security concerns grows. Transnational issues are proving to be more difficult to address than the bipolar rivalry of the Cold War. Few issues appear to have the luxury of time in which to be addressed and resolved. A greater emphasis on all-source collection management appears to be a strong necessity.

- **FINDING: There is still very little collection synergy among the intelligence collection stovepipes. As national security requirements become increasingly complex and demanding (transnational issues, short timelines), all-source collection management will be critical to future success.**

Production is, to some degree, taken as a given. Within production the lines as to what constitutes analysis is becoming increasingly blurred. Signals Intelligence (SIGINT) and Imagery Intelligence (IMINT) analysts do analysis: they analyze signals and images for contents and meaning. Much of their work is an internal IC function, often (although not always) destined to go from one analyst to another. But this is different than "all-source" analysis, the synthesizing of all available intelligence into a finished product, more clearly destined to go to a civil or military policy-maker. There is a great need to sort out these roles and give them clearer meaning within the IC and in relationship to one another.

- **FINDING: There is little IC attention given to production management. The line between SIGINT and IMINT analysis and reporting and all-source analysis and reporting is becoming increasingly blurred.**

In order to break down the collection stovepipes it is necessary to increase responsibility at the DCI level. If the various types of collection are not managed more coherently across the board, current problems will compound and efforts to achieve collection synergy and to improve all-source analysis will erode further. Such an approach is inherent in dealing with the IC as a more corporate entity. This should come under the DCI, with day-to-day responsibility falling to the DDCI/CM.

- **RECOMMENDATION: Under the DDCI for Community Management, create an IC-wide management organization responsible for directing all collection tasking (HUMINT and technical) to the appropriate agencies and ensuring a coherent, multi-INT approach to all collection issues.**

Similarly, the three technical collection activities (SIGINT, IMINT and Measurement and Signatures Intelligence -- MASINT) should stop being separate and competing agencies. They represent parts of a larger whole and should be managed as such. The link between the analysts who first receive information from the technical collection activities and the all-source analysts is crucial. However, there are other "exploiters" who can be housed directly with the all-source analysts. This would improve the synergy between collection and analysis, improve the all-source nature of analysis, and clarify blurring between different types of analysis and reporting. This can be done without putting at risk the unique services they perform for the military during time of war. Maintaining the designation of a "combat support agency," which currently applies to NSA, is appropriate.

- **RECOMMENDATION: Consolidate technical collection activities (SIGINT, IMINT, MASINT) and first-tier exploitation into a single agency -- the Technical Collection Agency (TCA).**

- **RECOMMENDATION: The TCA will be designated a Type-3 Combat Support Agency.**

- **RECOMMENDATION: The Director of TCA will be either a senior defense or intelligence civilian or three-star general officer.**

C. Technology Development Office. The IC has gone from being a leader in all aspects of technology crucial to its work, to being a leader in just a few -- primarily the technical collection systems but not the various types of data processing systems used to support them and other intelligence activities. As with all else in the IC, budget pressures are forcing rather difficult choices on managers across the entire range of activities. These pressures often lead managers to worry more about answering the immediate needs than to plan for the future. Research and development (R&D) funding is a victim of this mentality, as the immediate effects of deferring R&D are neither seen nor felt. However, given the strong dependence that the IC has on technology, this is an extremely short-sighted view. Several issues are at stake, among them: the ability of the IC to continue to be responsive to policy maker needs, especially in a world that is more politically complex and therefore requires a more flexible collection and processing base; rapid changes in information technology that offer the near-term possibility of increased production and increased synergy at decreased costs; and a necessary means of dealing with burgeoning sources of information, including an explosion of available open sources.

At the same time, the stovepipe mentality of the IC has also led to a situation in which there is duplication and increased costs that could easily be avoided. Commonality in items now as basic as data processing remain the exception rather than the rule. The net result of these trends is an IC that has gone from being a leader to one that looks increasingly antiquated.

- **FINDING: Tight budgets have squeezed R&D funding. The IC must manage R&D funding to ensure that the highest priority issues -- especially those requiring long lead times -- are being addressed and that there is no unnecessary duplication.**

There is unwarranted duplication in the IC's acquisition system for reconnaissance capabilities. The current system creates competition that exists more for bureaucratic reasons than for any developmental advantages. A merger of these responsibilities would also be a major gain.

- **FINDING: The IC's current system for acquiring reconnaissance capabilities has unwarranted duplication, creating competition for bureaucratic rather than developmental reasons.**

- **RECOMMENDATION: Create an intelligence acquisition agency to perform community research and development functions, called the Technology Development Office (TDO). TDO will comprise portions of the current NRO, Defense Airborne Reconnaissance Office (DARO), CIA/DS&T, et al.**

Some argue that such an organization will undercut the main strength of the NRO, its cradle-to-grave management of overhead systems. We believe that this view overstates the NRO's role, which is direct in terms of R&D and acquisition, but indirect in terms of the actual operation of these systems, which are carried out by contractors. We wish to emphasize the NRO's direct strengths.

National Intelligence Evaluation Council. The IC has not been very capable in terms of being able to evaluate its own intelligence process from end-to-end. This is, admittedly, a difficult task, in part because there seems to be little respite in which to do it. It is also difficult because there are few useful guidelines for assessing production. Customer surveys, although constantly used, are rather pointless. Self-assessment is, at best, difficult. IC managers are constantly hard put to answer: "What is the value added of intelligence to the policy process?" The fact that the question is asked at all is troublesome. The fact that it cannot be answered is worse.

This type of evaluation is an extremely important task. Without being able to assess whether or not tasking and collection respond to policy-maker requirements, whether analysis is making the best use of resources, the IC process becomes rather pointless. It appears to move more on inertia rather than on need. Being able to do better is now even more important as resources either remain stable or shrink. Without a better feel for the weak points and strong points across the *entire* IC process, all parts will likely suffer, as will the contribution of intelligence to policy making.

- **FINDING: The IC needs to improve its ability to evaluate the intelligence process from end-to end, *i.e.*, to be better able to relate requirements, tasking, collection and production.**

The IC already has an office charged with evaluations, as part of the National Intelligence Council (NIC). This appears to be the logical group to charge with the broader types of evaluation responsibilities noted above. Consonant with its new mandate, this staff should be separated from the NIC and made a National Intelligence Evaluation Council (NIEC) in its own right. The remaining part of the NIC, *i.e.*, the National Intelligence Officers (NIOs), would become part of the new CIA, as noted above. The head of this new council would be appointed by the DCI, as is the current head of the NIC, and would report directly to the DCI, so that the DCI can readily oversee and assess the entire intelligence process.

- **RECOMMENDATION: Establish a National Intelligence Evaluation Council (NIEC) to evaluate IC-wide collection and production, and to interact closely with the requirements, collection management and resource management functions of the CMS.**

- **RECOMMENDATION: The head of the NIEC will be appointed by and report directly to the DCI.**

Civilian Intelligence Reserve Program. The ability to "surge" analytical resources and to capitalize on expertise residing outside of the IC will be key to the effectiveness of the IC as it enters the 21st Century. No requirements process can predict all of the issues that are likely to be of paramount interest to policy-makers in the course of any year. Surveys are, by and large, not useful to policy-makers. As Lt. General Brent Scowcroft observed, senior policy makers do not know what they need from the IC until they need it. In a national security environment where there is not one predominant focus, as was the case during the Cold War, flexibility becomes a central necessity for the IC. As one of our witnesses, Ambassador Robert Kimmitt, former Under Secretary of State for Political Affairs, has stated, the IC will have to be an inch deep and a mile wide, with the ability to go a mile deep on any given issue. To do this, the IC must maintain some level of knowledge on all nations/issues at some level of detail -- an intelligence "base."

- **FINDING: The IC must be able to "surge." As Ambassador Robert Kimmitt put it succinctly, IC coverage must be an inch deep and a mile wide, with the ability to go a mile deep on any given issue.**

- **FINDING: The IC will be required to maintain some level of knowledge on all nations/issues at some level of detail -- an intelligence "base." The capability to support this base or to "go a mile deep" need not be self-contained within the IC.**

The CIA already has in place procedures enabling it to increase its capabilities, using former employees on a temporary basis. This capability should be augmented into an IC civilian reserve program, in which experts not in the IC (in academia, business, etc.) can be kept on retainer both to provide ongoing information on warning and trends and to be utilized during crises to augment IC assets. Such a program has several advantages. First, it allows the IC to concentrate on the current areas of highest priority and concern while knowing that someone who is attuned to IC needs is also keeping an eye on areas that are quiescent. Second, the ability to bring in experts who understand local politics and players in a region is especially important during the early phase of a crisis, when the IC is often scrambling to come up to speed. Many of these experts can be kept on retainer and be asked to do unclassified work, that, in effect, will provide the IC with more knowledgeable access to the open sources. If the "reservists" are asked to work within the IC for extended periods, then some thought has to be given to the issue of clearances and polygraph requirements. A flexible approach to these issues would best serve the overall interests of the IC and the nation.

There are many ways a civilian reserve program could be run. To be successful, however, such a program would probably have to be developed and managed at the Community level, so as to properly address administrative concerns (security, pay, etc.) as well as substantive concerns -- assuring that duplicative expertise is minimized and agencies do not compete for resources to support individual reserve programs. Some developmental work on a reserve program is being done at this time in the NIC. This work should continue and a pilot program should be enacted in the near term.

- **RECOMMENDATION: An IC-wide civilian reserve program should be established, whose participants can provide ongoing trends and warning information and can be utilized to "surge" as part of the IC, thus augmenting existing IC assets, especially during crises.**

Congressional Oversight. *IC21* also examined the way in which Congress handles its oversight responsibilities for intelligence. Although these findings and recommendations would not require formal legislation, they would require changes in the rules of the House.

The current oversight system is 20 years old, a direct product of major congressional and executive branch investigations that revealed a number of shortcomings in both how the IC functioned and in how Congress pursued intelligence oversight. This is important to note as it helped foster the view that intelligence and intelligence oversight were in some ways extraordinary issues, to be handled in amanner different from other government functions. Not surprisingly, we believe that the current oversight system has responded well to these concerns.

- **FINDING: The current Congressional oversight system is a product of extraordinary disclosures of the 1970s and their sequels. It has responded well to the concerns that fostered it.**

Having said that, we are also aware that this continuing view of intelligence as something extraordinary also puts pressures on intelligence oversight that are unique. All oversight is a mixture of two roles: investigator and advocate. Being an advocate for intelligence may be more difficult than for other government functions not only because of the secrecy that is involved, which limits what can be said, but also because of the ongoing suspicion about intelligence agencies and activities in some quarters. Several former DCIs pointed out that intelligence, unlike other federal programs, has no natural constituency. Therefore, if Congress is not prepared to act as an advocate when that role is proper and necessary, no one else will. This aspect of oversight is especially important if the IC and its necessary activities are to enjoy even a minimal amount of public support.

- **FINDING: Oversight embodies two roles: investigator and advocate. HPSCI advocacy for the IC is essential but difficult given the secret nature of intelligence. Intelligence, unlike other federal programs, has no natural constituency; therefore, Congress plays a vital role in building public support.**

As with all oversight, there is an inherent tension between the amount and type of intelligence information that Congress believes it needs and what the Executive is willing to provide. In the case of intelligence, this is exacerbated by the perception that Congress is the major source of leaks.

- **FINDING: Existing oversight identifies and continues to address problems within the IC. Inherent tensions between executive and legislative branches cause resistance to the free flow of information to the Congress. This is exacerbated by the perception that Congress is the major source of leaks of classified information.**

A joint committee on intelligence has been suggested as one remedy. We do not believe that it would substantially reduce the number of Members and staff with access to classified information. The House and Senate Intelligence Committees also do not pursue identical agendas. Given the breadth and diversity of the IC, this two committee oversight structure is a strength, as it broadens oversight. A joint committee would reduce the effectiveness of the current checks and balances. Finally, it would continue to underscore the view that intelligence is so different that it must be handled in an extraordinary manner.

- **FINDING: A joint intelligence committee would not improve the quality of oversight and would erode existing legislative checks and balances. It would reinforce the perception that intelligence oversight is different and that intelligence programs require different levels of scrutiny.**

Dealing with the intelligence budget raises some problems. As the IC budget is classified -- both the overall figure and virtually all of the component parts -- it is masked by being made part of the defense budget. Intelligence, in the House is authorized separately, and then appended to the defense authorization. Should that budget become subject to reductions, the intelligence budget often has to give its "fair share," not for reasons inherent to the value of intelligence programs, but largely because of this budget mechanism. This puts intelligence at a disadvantage.

Within the appropriations process, intelligence is dealt with in the National Security Subcommittee. This also can result in intelligence being dealt with as an appendage of defense issues rather than as a separate government function. This process also results in a confused Congressional message on intelligence because of the variety of reasons for which budget decisions may be made.

- **FINDING: The current Congressional budget process puts intelligence programs at a disadvantage, making them subject to arbitrary cuts because the intelligence budget is subordinated to the defense budget.**

- **FINDING: The current budget process can also result in a confused Congressional message to the IC.**

A major facet of the way in which the current intelligence oversight system was created is the requirement that tenure on HPSCI be limited. This rule was adopted because it was felt that past Congressional overseers had become too close to the IC agencies over prolonged periods of time and had lost a certain critical objective edge. Twenty years later, the costs of such a system are also apparent: a rapid turnover in membership and in some senior staff, diluting the capabilities of the Committee. There have been six chairmen of HPSCI over the last six Congresses. The oversight system is now sufficiently mature to allow, at a minimum, an extension of the tenure rules and serious consideration of ending tenure limits.

Similarly, thought should be given to changing the Committee from a select committee to a standing committee. Again, this raises important questions, including the degree to which this will be an attractive assignment; the continued utility of having "cross-over" Members, particularly from Appropriations; and whether it is better to have the Speaker make appointments to the Committee or leave it to the majority caucus.

- **RECOMMENDATION: The House should give serious consideration to either extending or removing tenure limits on HPSCI.**

- **RECOMMENDATION: The House should consider making HPSCI a standing committee, with appointments still made by the Speaker.**

VI. Findings and Recommendations: Non-Legislative

As noted above, the *IC21* staff studies made numerous findings and recommendations that would not require legislative action. We believe that these will also support the findings and recommendations made above, improving the overall performance of the IC. They are listed here with brief introductions as to the nature of the issues being addressed. Broader and more detailed discussions can be found in the staff studies themselves.

Intelligence Community Management: Production. Production is, in effect, the end of the intelligence pipeline. It is what the policy makers see, a product (usually written), drawn from the various pieces of collected intelligence and leavened by the analyst's own knowledge and experience.

We must face the fact that analytical resources are unlikely to grow substantially. Although the decline of the past several years in intelligence budgets was halted in 1995, there is no guarantee that this is much more than temporary relief. Moreover, it is not likely that there will be large increases in intelligence spending over the next several years. Therefore, the IC needs to manage smarter, finding new ways to do more with less. Ongoing rapid technological change in information management may offer new possibilities and advantages. The ability to move information, including intelligence, between and among disparate and widely-separated work stations could increase synergy above the actual number of current analysts. Linking analysts of all sorts in this manner may also be helpful, in effect creating a "virtual analytical environment."

- **FINDING: Analytical resources are unlikely to grow substantially. Increased and more synergistic productivity may be possible through the use of a "virtual analytical environment."**

- **RECOMMENDATION: Create a "virtual analytical environment" within the IC that electronically links collectors, exploiters, analysts and customers, as appropriate, and maximizes the productivity and responsiveness of individual analysts.**

Intelligence Community Management: Programming and Budgeting. We envision that the DCI will execute most of his authority over the NFIP (and the broader IC budget) through the CMS, under the DDCI/CM. It is essential that this staff have

both program analysis and evaluation capability and comptroller capability if these responsibilities are to be carried out effectively. These capabilities will also be meaningless unless there is also the authority to withhold funds.

- **RECOMMENDATION: The CMS should have a program analysis and evaluation (PA&E) capability and a comptroller capability, with the authority to withhold funds.**

Understanding or managing the IC is complicated by its rather rigid and stratified budget structure. Each asset, activity or program is allotted to one and only one IC responsibility. This makes it very difficult to achieve synergies from collection systems, processing and even analysis. It also tends to skew the IC budget, giving even greater emphasis than is the actual case to defense-related activities, which of necessity remain dominant. It is important to understand that most IC assets and activities fall into multiple categories and should be tracked accordingly. This would create a capability that is currently lacking: being able to ascertain rapidly and with some assurance of accuracy what part of IC resources is devoted to specific issues, such as non-proliferation, East Asia, etc.

- **RECOMMENDATION: An IC programming, budgeting and accounting system must be developed that allows the IC to build budgets and track expenditures in multiple categories.**

Intelligence Community Management: Personnel. To repeat, people are the key element of the IC. All of the collection capabilities are meaningless machines unless there are dedicated people behind them -- building them, operating them, processing the data, analyzing it.

We find that the vast majority of people who work in the IC are extremely dedicated to their work and to its value to our national security. The system within which they work, however, is not designed to get the very best out of them in terms of either bureaucratic rules or the type of leadership (rather than management) that breeds elan.

Curiously, the IC tends to manage personnel much like it manages collection, through an array of "stovepipes" that are bundled together but are not well inter-connected. It is very difficult for either managers or analysts themselves to move about within the IC.

- **FINDING: In order to create a more corporate culture and reduce the stranglehold of stovepipes, the barriers to lateral movement within the IC need to be broken down.**

- **FINDING: The IC requires personnel reform to enable it to change its skill mix and to streamline its workforce in an era of reduced government spending.**

- **FINDING: Improving the personnel system will improve morale, public relations and accountability.**

- **RECOMMENDATION: Implement the recommendations of the Jehn Report.**

- **RECOMMENDATION: Standardize the SES system within the IC, and strongly encourage rotational assignments as a prerequisite for SES rank. Include rotations to industry as part of the IC rotation system.**

- **RECOMMENDATION: Introduce legislation, coordinated with OMB, to authorize a pilot program to reduce the number of IC personnel further, to include lifting of the 2% waiver and directed retirement of retirement-eligible personnel.**

Intelligence Community Management: Research and Development. Under the corporate concept we advocate, the DCI should be responsible for adapting advanced technology to IC needs on short notice. At two different full Committee hearings we were struck by expert testimony decrying the inability of the government to move quickly to purchase technology on a timely basis. The DCI needs a better mechanism to find short-cuts in this process.

- **FINDING: The DCI needs a mechanism to fund good technology ideas on short notice. Venture capital concepts should be part of this process.**

A glaring example of current IC problems is information systems. There is a veritable plethora of systems, standards and acquisition processes. If we are going to move towards an IC that has greater inter-operability among its disparate parts, and tries to achieve "virtual analytical communities" tied together electronically, then a common system is a bedrock requirement.

- **FINDING: The IC needs greater standardization of information systems, including acquisition by a single organization. There also needs to be a budgetary mechanism to recapitalize these systems cyclically to keep everyone interoperable and up-to-date.**

- **RECOMMENDATION: Centralize planning and budgeting for IC R&D, to include administration of the National Technical Alliance with the National Imagery Display Lab and the National Media Lab.**

- **RECOMMENDATION: Establish a Military Exploitation of Reconnaissance and Intelligence Technology (MERIT)-like program for the IC to fund "good ideas" and to exploit technological targets of opportunity. The DCI should also use his Contingency Reserve Fund for such opportunities.**

- **RECOMMENDATION: Centralize development of standards and protocols for the IC. Establish a budgetary mechanism for rapid and continuous update of information systems and automation technologies.**

Intelligence Community Requirements. Intelligence is a service. Its entire *raison d'etre* is to provide a product to or undertake operations for other parts of the government. Unless the IC is responding to policy maker requirements, it simply is not doing its job. Requirements are the prime cause of all other IC activities: they drive collection, tasking, analysis and determine the allocation of resources throughout these processes. Getting control of requirements is fundamental and urgent.

The requirements process has traditionally been one of the most vexing aspects of intelligence management. Ideally, intelligence producers would like to have guidance from the highest policy makers possible. The interagency process, which includes the IC, informs the IC as to policy maker concerns. Over the years the process has been haphazard and imperfect.

The world of the late-20th and early-21st centuries presents new stresses for the requirements process. A Cold War-based IC had the comfort of knowing that its major emphasis was the struggle with the Soviet Union and all that this entailed. The absence of this overwhelming requirement has resulted in a growing tangle of new requirements, none of which has the same lasting primacy. Issues are the "highest priority" for rather short periods of time. At the same time, the resources available to the IC to deal with current and new requirements continue to decline. The need for a better requirements system is clear.

- **FINDING: The IC needs an overarching concept for coordinating intelligence requirements, especially when faced with declining resources, a growing customer base, and increasingly diverse requirements.**

- **FINDING: The IC needs a corporate understanding of its collection and production capabilities and how it uses these resources to meet intelligence requirements. The IC also needs a strategic vision outlining what resources will be needed in the 21st century to fulfill likely intelligence requirements.**

- **FINDING: Presidential Decision Directive 35 (PDD-35) has focused the IC on important near-term, high priority requirements. However, PDD-35 has begun to drive intelligence collection and production at the expense of lower "tier" issues.**

- **FINDING: The IC's ability to maintain an intelligence "base" on many lower tier issues is threatened not only because of PDD-35's unintentional effect on collection and production, but also because the IC currently has no mechanism to ensure a basic level of coverage on "lower tier" countries.**

- **RECOMMENDATION: The IC should fulfill PDD-35 requirements, but also maintain the capability to have a basic level of worldwide coverage.**

- **RECOMMENDATION: The DCI should direct the CMS to devise a strategic plan, which should be updated yearly if necessary, outlining national security issues and gaps that the IC will likely face 10 to 15 years into the future.**

- **RECOMMENDATION: The National Intelligence Evaluation Council (NIEC) should be responsible for the Comprehensive Capabilities Review. The review should be updated continuously, taking the DCI's strategic plan into account, to assess the IC's worldwide collection/analytical capabilities and gaps against all tier issues.**

- **RECOMMENDATION: The IC should implement a "virtual analytic environment" to link collectors, exploiters, analysts and customers electronically, as appropriate, to improve the IC's responsiveness to customer needs. DIA's test-bed plan, JIVA (Joint Intelligence Virtual Architecture), is a useful place to start.**

- **RECOMMENDATION: Intelligence managers should function less as intermediaries who control the information flow to and from policy-makers and more as facilitators who ensure that valid requirements are fulfilled with appropriate resources. Managers should also ensure that intelligence does not become politicized as a result of the close policy-maker/analyst working relationship.**

Collection Synergy. Once requirements have been established, the next major decision is the allocation of resources to meet these requirements, especially the resources required to collect needed intelligence.

No other nation has collection capabilities comparable to those of the United States. In terms of breadth and depth, the United States has enjoyed a vast superiority as the result of major investments and a great deal of hard work.

Intelligence experts speak to one another about collection disciplines, *i.e.*, the basic groups into which collection fall:

SIGINT: signals intelligence;
IMINT: imagery;
MASINT: measurement and signature intelligence;
HUMINT: human intelligence; and, most recently,
OSINT: open sources.

These five groups have not developed evenly and are not managed in similar manners. Ideally, they should provide an array of information, allowing analysts to confirm intelligence gleaned from one discipline by comparing it with that gathered from others -- creating a true synergy. Each discipline has particular strengths and weaknesses, working better or worse than others against particular intelligence problems. Together, it is hoped that they will minimize uncertainty and amplify that which is known.

As managed today, there are impediments towards achieving this synergy. Among the most obvious is the problem of stovepipes, the fact that each discipline is managed with a great deal of independence from the others. As noted above, rather than being allies, they become competitors, especially when intelligence budgets are being developed. This internecine competition undercuts much of the hoped-for synergy and can become increasingly debilitating.

- **FINDING: The U.S. has derived tremendous benefit from a balance and interaction among the three technical intelligence disciplines (SIGINT, IMINT, MASINT), HUMINT and open sources. However, the IC has not managed collection consistently across the various INTs, thereby decreasing efficiency and productivity.**

- **FINDING: This benefit could erode unless greater attention is given to closer central management and coordination among all INTs.**

- **FINDING: Recent international and political changes and technological advances have greatly increased the quality and quantity of open source information.**

- **FINDING: "All-source" analytical skills are central to future intelligence capabilities and need increased emphasis.**

- **RECOMMENDATION: A CMS with IC-wide authority over, and coordination of, requirements, resources and collection would greatly aid collection synergy.**

- **RECOMMENDATION: To the extent possible, there should be common standards and protocols for technical collection systems, from collection through processing, exploitation and dissemination.**

- **RECOMMENDATION: The IC must continue to develop improved means of collecting, exploiting and processing open source information. There must be a concerted effort to educate intelligence producers and consumers regarding the utility of open source information.**

- **RECOMMENDATION: The IC must improve its ability to retrieve data from common databases. These databases must be checked thoroughly by those responsible for requirements and analysis before new collection tasks are levied. Collection should be guided by the use of the least costly, most efficient and most productive means, whether overt or covert.**

Collection: Launch. Spaceborne technical collection systems are useless unless there are adequate means of putting them into orbit. It is a truism, worth repeating, that launch vehicles must be considered a critical part of our overall intelligence collection architecture.

- **FINDING: Launch vehicles will remain a critical component of the U.S. intelligence collection architecture.**

- **FINDING: The U.S. needs simple, reliable, affordable launch vehicles. The Titan-IV launch vehicle is not the best means of ensuring a viable 21st century collection architecture. Other options -- such as new launch vehicles and changes in satellite design -- must be pursued.**

- **FINDING: Current launch vehicles are becoming prohibitively expensive.**

- **RECOMMENDATION: If technically feasible, all IC payloads should be taken off the Titan-IV. No Titan-IVs should be purchased by the IC after the 1997 buy, and even that should be reconsidered.**

- **RECOMMENDATION: The U.S. should examine the viability of advanced technologies to reduce the size of satellites.**

- **RECOMMENDATION: The Air Force should modify its Evolved Expendable Launch Vehicle (EELV) program to focus solely on the heavy lift problem. The U.S. government should take advantage of the Medium Launch Vehicle (MLV) competition between McDonnell Douglas and Lockheed Martin in order to keep MLV costs low.**

- **RECOMMENDATION: All IC payloads, during their current redesign phase, should incorporate the "ship and shoot" approach (*i.e.*, payloads arrive at the launch site ready for launch, with no on-site assembly, testing, etc.).**

- **RECOMMENDATION: All IC payloads, during the current redesign phase, should conform to the standard interface of the launch vehicle. NRO MLV class payloads should be compatible with both the Atlas IIAS/R and the Delta 3.**

Technical Collection: SIGINT, IMINT, MASINT. Detailed discussions of these collection disciplines and plans for future capabilities are, of course, highly classified. However, there are broad points at issue that can be discussed on an unclassified basis.

SIGINT. SIGINT is an extremely valuable capability, allowing the observation of activity through the content and pattern of signals and giving insights into intentions. It is responsive to a large number of the issues with which the IC is now dealing and will continue to do so into the foreseeable future.

- **FINDING: SIGINT provides a valuable capability both to observe activity and to gauge intentions. It will continue to be a critical element of the IC for the foreseeable future.**

- **FINDING: The SIGINT system performs well, but is at a crossroads. The proliferation of digital communications, fiber optic cable, sophisticated encryption and signalling techniques are major technical challenges, both for collection and processing. Growth in one telecommunications medium does not detract from the others; all types of communications are increasing. The ability to intercept all of these media is important for several reasons: different types of information use different communications media; pieces of the same message may travel different routes; multi-source collection makes deception by current or potential adversaries more difficult.**

- **FINDING: SIGINT is already the most expensive of the collection disciplines. Balancing the required level of investment in technology with the maintenance of existing core capabilities is the true challenge for SIGINT in the 21st century.**

- **RECOMMENDATION: Improve the management and focus of SIGINT R&D to ensure that critical areas are adequately funded.**

- **RECOMMENDATION: Mandate a review of the overall Electronics Intelligence (ELINT) architecture and the mix of available collection platforms.**

- **RECOMMENDATION: Examine the feasibility of smaller platforms to reduce the cost of certain collection.**

- **RECOMMENDATION: Continue to press for a unifying policy on Information Warfare (IW) from the Administration. Clarify the management and direction of offensive IW activities in peacetime and in support of military operations.**

- **RECOMMENDATION: Reduce numbers of different airborne SIGINT platforms while increasing overall numbers of aircraft; develop and implement a common ground processing architecture for airborne SIGINT operations. Develop SIGINT payloads for use on Unmanned Aerial Vehicles (UAVs).**

IMINT. The utility of imagery will continue both for those issues with which it is most often associated -- indications and warning, and military operations -- but also for many of the transnational issues that appear to be increasingly important in the late 20th century.

- **FINDING: IMINT will continue to be an important collection discipline for a wide variety of issues: indications and warning; support to the military; and monitoring arms control agreements, refugee flows, narcotics cultivation and ecological problems.**

- **FINDING: Given present trends, the number of images collected will continue to outpace our ability to analyze them.**

- **FINDING: Collection costs continue to rise at the expense of processing and exploitation.**

- FINDING: Imagery analysts are working with archaic tools; the current acquisition process does not facilitate the timely infusion of new technology.

- FINDING: The imagery community is badly fragmented. Any restructuring should be considered only within the wider context of all other intelligence functions and activities.

- FINDING: "Denial and deception" activities by foreign governments are a current problem. As U.S. imagery capabilities become more widely known, this problem will likely grow.

- FINDING: The IC can use commercial imagery more effectively to meet some requirements.

- FINDING: Imagery dissemination to the military below the Joint Task Force level remains a problem.

- FINDING: The imagery community is not currently able to satisfy the requirements for both immediate and detailed analysis.

- RECOMMENDATION: The IC must improve its acquisition and use of commercially-available imagery. Such imagery can be used in lieu of more costly national assets. As demands to share imagery with non-Allies during multilateral operations increase, the use of commercial imagery is especially important to obviate security concerns.

- RECOMMENDATION: Set up an account for the easy purchase of commercial imagery, done under common U.S. government licenses. A central repository and indexing system should be created for easy access by all users.

- RECOMMENDATION: The IC must move to all-digital exploitation of imagery, with access to cross-INT databases. Move to a "virtual analytic environment," i.e., one in which analysts are connected electronically. Increase funding to accelerate the procurement of softcopy (digital) workstations for imagery analysts.

- RECOMMENDATION: The IC should move aggressively to infuse new technologies, such as automatic target recognition capabilities, in order to help streamline the imagery exploitation process.

- **RECOMMENDATION: Expand the purview of the National Technical Alliance, increasing its resources and flexibility to provide more rapid fielding of new technologies, and to exploit commercially available technology.**

- **RECOMMENDATION: The IC must continue to examine and to field means by which to overcome "denial and deception" activities.**

MASINT. MASINT -- measurement and signals intelligence -- is undoubtedly the least understood of the various collection disciplines. This is unfortunate, both for its own sake and because MASINT will continue to be an important source for military planners, during military operations, and for monitoring arms control and proliferation activities.

- **FINDING: MASINT, as a specific and unique discipline, is not well understood by either the IC or policy consumers. Therefore, the potential of its future contributions, particularly to tactical applications, may be limited.**

- **FINDING: MASINT will become increasingly important in providing unique scientific or highly technical information contributions to the IC. It can provide specific weapon identifications, chemical compositions and material content and a potential adversary's capability to employ weapons.**

- **FINDING: The Central MASINT Office (CMO) has the requisite legal authorities to carry out its responsibility of managing MASINT. However, it is not staffed commensurate with its responsibilities, and a fractured organizational structure limits its overall management abilities.**

- **FINDING: MASINT is a science intensive discipline that needs personnel well-versed in the broad range of physical and electrical sciences. Such personnel cannot typically be professionally developed within the IC. They must come from academia fresh with the scientific knowledge from experimentation and research. Nor can they continue to be proficient in their areas of expertise if they are maintained in government employ for an entire career.**

- **RECOMMENDATION: The IC should create a U.S. MASINT System analogous to U.S. SIGINT and U.S. IMINT Systems (USSS and USIS).**

- **RECOMMENDATION: The MASINT manager should be a general officer or SES, and should be a member of the Military Intelligence Board, National Foreign Intelligence Board and other senior DCI and DOD boards and panels. His authorities to manage MASINT should be on par with those of the SIGINT and IMINT managers.**

- **RECOMMENDATION: Training is critical. The IC needs to increase emphasis on informing the IC and consumers about MASINT capabilities and products. Additionally, the IC needs to make MASINT a formal course of professional education for all IC school houses.**

- **RECOMMENDATION: The IC should examine the feasibility of pursuing trial personnel management programs that provide incentives to recruit the necessary scientific experts. Such experts may not spend a 20-30 year career in government employ.**

Clandestine Service. In addition to the legislative proposals for the CS described above, there are other management issues that need to be addressed. These include civilian and military personnel management, the CS's role in operations, and the management of operations overseas.

- **RECOMMENDATION: The IC's personnel system should ensure the recruitment of highly qualified junior employees, the development of technical clandestine operators and managers, and the aggressive removal of marginal and unsuitable employees.**

- **RECOMMENDATION: The military cadre of the CS should consist of military clandestine operations officers having a viable military career track within that specialization and of the same high professional and personal qualifications as the civilian cadre.**

- **RECOMMENDATION: The DCI needs to reaffirm and reiterate throughout the IC his designation of the CS's role to lead the IC in its conduct of foreign "clandestine operations," *i.e.*, espionage, counter-espionage, covert action and related intelligence liaison activities abroad.**

- **RECOMMENDATION: The CS's Chiefs of Station should act as the U.S. Government's on-site focal point for the deconfliction of all intelligence and law enforcement activities abroad, with an appeal process functioning through the Ambassador and/or a Washington-based interagency mechanism.**

- **RECOMMENDATION: The CS should have at least a minimal presence in most countries (a "global presence") so as to maintain a broader base-line contingency capability and to respond to transnational collection requirement.**

- **RECOMMENDATION: The management of clandestine operations requires an extraordinarily high level of management attention, operational expertise and coordination. Managerial and personnel assignments must be consistent with this fact.**

IC "Surge" Capability. Unpredictability is one of the facts of life of any intelligence system. No requirements process will be able to predict all of the issues that are likely to be of paramount interest to policy-makers in the course of any given year. Indeed, flexibility of all resources -- technical and personnel -- are necessary in order to respond quickly to new events. This problem of requirements and resources has been made increasingly difficult in the post-Cold War world. The end of the Cold War not only removed the single overwhelming focus of the IC, but also contributed to a breakdown of international order in specific regions, particularly the growth of ethnic warfare, and exacerbated a number of transnational issues.

The ability of the IC to "surge" resources -- *i.e.*, to focus collection and analysis, and sometimes operational capabilities -- on suddenly important areas, is of increasing importance. One of the witnesses at an *IC21* hearing, Ambassador Robert Kimmitt, former Under Secretary of State for Political Affairs, put it succinctly when he said that IC coverage must be an inch deep and a mile wide, with the ability to go a mile deep on any given issue.

- **FINDING: The ability to meet future challenges effectively will require: increased internal operating efficiencies; a more collective, corporate approach toward utilization of resources; and structured programs that provide continuous force augmentation and "surge" capability.**

- **FINDING: A flexible, dynamic and well-planned surge capability must be developed that can be relied upon both day-to-day and during crises.**

- **RECOMMENDATION: Development of more flexible collection capabilities should not only include moving to smaller satellites, but also to developing and incorporating "tactical" satellites that would allow for a "surge" in collection capability for specific crises.**

- **RECOMMENDATION: The DCI's ability to establish IC Centers and Task Forces quickly (including the rapid transfer of personnel and resources throughout the IC) must be enhanced and should include the ability to bring "surge" resources into the IC from other areas.**

- **RECOMMENDATION: Better utilization of existing military reserve components is also required. Consideration should be given to placing some of these components under the DMI for better utilization during time of need.**

Support to Military Operations. Support to military operations (SMO) is one of the major roles of intelligence. Some argue that it is *the* major role of intelligence. The Clinton administration -- both policy makers and senior intelligence managers -- has stated that SMO is *the* top priority for intelligence. Critics question why this statement is necessary, given that much of the IC's effort has always been shaped around this specific intelligence role and that, in the post-Cold War world, U.S. national security is actually less threatened than at any time since 1940.

This debate over SMO is important as it goes to the heart of both requirements and resources. Intelligence is not an easily expanded resource. As noted in the discussion on the IC's ability to surge, covering current requirements and taking steps to address unexpected ones is difficult at best. The more resources devoted to any one area, the fewer there are left to address others. The issue is not whether the IC should devote resources to SMO, but rather how much SMO is reasonable given other, competing demands on a fiscally constrained IC.

SMO is, to some extent, a contingent need. At least through the Cold War, U.S. defense policy had been shaped around the idea of deterring combat, of using force as a last resort. Other, non-SMO, policy needs are current -- diplomacy, narcotics, terrorism, proliferation. Thus, a balance needs to be struck. Urging an increased emphasis on SMO without looking across the board at all IC requirements runs the risk of leaving many other ongoing policy needs partially or completely unfulfilled.

- **FINDING: The current demands being placed on the IC to support military operations will make it difficult for the IC to meet the broader national security challenges of the 21st century.**

- **FINDING: Currently, SMO demands are being satisfied at the expense of maintaining the necessary intelligence"base" that will be critical to the IC in addressing future national security needs.**

- **FINDING: Maintaining both the "base" and SMO represent valid concerns. SMO requirements must not stand alone, apart from other intelligence requirements.**

- **FINDING: The IC must develop and maintain a balanced approach in satisfying these concerns. The IC must ensure that the "base" is maintained even during periods of crisis, when IC resources can easily be overwhelmed by all-consuming SMO requirements.**

- **FINDING: The new operational strategy, Dominant Battlefield Awareness, will require significant advances in technology, development of consolidated requirements, coherent tasking management and synergistic intelligence collection capabilities. It is necessary to give serious thought to the amount of IC resources likely to be available to support such strategies.**

- **FINDING: Emphasis on concepts such as "sensor-to-shooter" have promoted the dissemination of intelligence data and products to the lowest level of military operations, without full consideration of the effect on the "warfighter."**

IC Centers. The IC began using centers in 1986 as a means of addressing certain long-term issues on an IC-wide basis. At present there are seven such centers, covering the issues of arms control, non-proliferation, terrorism, counterintelligence, counternarcotics and organized crime, and overseas security.

IC21 examined the concept of centers with a view towards determining whether they represented a better way to organize IC efforts, or if they were merely an organizational fad. Moreover, if they were a better concept, what implication did this have for the more traditional offices in CIA and the other major intelligence agencies? We concluded that this concept was successful in addressing specific, enduring issues and serving as IC focal points for these issues. Indeed, it would appear that centers will be even more important in an IC that puts greater emphasis on corporate management concepts.

- **FINDING: Centers are successful in addressing critical, enduring intelligence issues on an IC-wide basis and should continue to be used as necessary.**

- **FINDING: There are several types of centers; they do not all perform the same functions.**

- **FINDING: IC-wide representation within Centers is insufficient and must be increased.**

- **RECOMMENDATION: Centers should be subject to a mandatory five year "sunset" review process under the DCI's direction.**

- **RECOMMENDATION: The Directors of the Nonproliferation, Crime and Narcotics, Counterterrorist, National Counterintelligence and Arms Control Intelligence Staff (renamed the Arms Control Intelligence Center) should also serve as IC issue managers.**

- **RECOMMENDATION: Although the center directors will serve as issue managers within the CIA, the centers should be located and managed within the IC based upon their unique attributes and principal roles:**

  The National Counterintelligence Center functions principally as a policy and coordination body and should continue to come under the NSC.

  The Arms Control Intelligence, Nonproliferation, and Crime and Narcotics Centers should come under the CIA.

  The Counterterrorism Center and the Counterintelligence (renamed the Foreign Counterintelligence) Center should come under the CS.

  The Center for Security Evaluation should come under the ISO.

- **RECOMMENDATION: To facilitate IC participation in centers, the IC should develop a consistent policy regarding reimbursable billets and reimbursement of travel expenses. An appropriate amount of money should be designated in the authorization specifically to fund these center expenses.**

- **RECOMMENDATION: The IC personnel evaluation and promotion systems must accurately reflect and reward the performance of employees detailed to centers.**

Intelligence and Law Enforcement. One of the hallmarks of those transnational issues that have moved to the top of the IC agenda in the post-Cold War world is that they tend to straddle intelligence and law enforcement concerns. Concerns about safeguarding fundamental civil liberties have dictated a strict division between these two spheres. For example, the National Security Act mandates that the CIA will have no "police, subpoena, law-enforcement powers, or internal security functions."

Issues such as narcotics, crime, terrorism and proliferation make the maintenance of this division more difficult. Having said that, it would appear that current provisions in law and in executive orders are sufficient to maintain the necessary difference without impeding the kind of cooperation between intelligence and law enforcement that most believe is necessary.

- **FINDING: The National Security Act and existing Executive Orders are sufficiently flexible to allow improved cooperation between law enforcement and intelligence without blurring the important distinctions between the missions and authorities of the two communities.**

- **FINDING: Increased joint training is essential to closer cooperation and coordination between the two communities.**

- **RECOMMENDATION: Congress should consider statutory or other language that will set forth "reasonable" expectations of IC reporting on criminal activities.**

- **RECOMMENDATION: Within law enforcement agencies, information management and policies must be improved to facilitate sharing appropriate information with the IC that has been collected during the course of law enforcement investigations.**

- **RECOMMENDATION: Each law enforcement agency should be responsible for its own coordination with the CS.**

IC Communications. The relationship between communications and intelligence has been a difficult one for the U.S. government. The two functions have a certain degree of inter-relationship based on the need to be able to pass intelligence from collectors to analysts and from analysts to policy consumers on a timely basis. Some have even suggested that this is *the* critical problem in disseminating intelligence.

It is important to distinguish between the two related but different parts of this issue. The IC is responsible for *dissemination*, the actual movement of intelligence products to their intended audience among policy makers. However, the technical or physical *means* by which this dissemination occurs are not and should not be responsibilities of the IC.

- **FINDING: Communications is often cited as the most critical problem in disseminating information to users in a timely fashion. Timely delivery of intelligence products to consumers in the proper form is generally an intelligence weakness.**

- **FINDING: The IC is responsible to its consumers for timely <u>dissemination</u> of its products in the required forms and format. The development, procurement, management and maintenance of <u>communications</u> needed to disseminate these products are not, and should not be core competencies for the IC.**

  "Communications" is defined narrowly as the <u>conduit(s)</u> for moving data from one point to another. This includes the <u>standards</u> necessary to interface hardware and software at either end of the communications conduit.

- FINDING: The communications community is best suited for providing specific standards and interface protocols to communications users to ensure interoperability. It is also best suited to provide the majority of U.S. government communications paths.

- FINDING: Managing Command, Control and Communications (C3) with intelligence in Defense, amalgamates these two activities, to the general disadvantage of intelligence, which tends to get shorter shrift and is overwhelmed by the much larger communications presence.

- RECOMMENDATION: The IC should not have communications as a core competency. It should be a communications user, with specifically identified requirements, and should not directly contract for communications "bandwidth."

- RECOMMENDATION: The IC must complete a thorough study of total IC communications needs and provide the results to the communications community. Such a study must be continuously reviewed and updated as new requirements emerge and as new capabilities and technologies are brought into service.

- RECOMMENDATION: The IC should maintain a consolidated core of communications professionals whose primary tasks will be to act as the "technological knowledge bridge" between the providers and the IC, to define communications standards for the IC and to review current capabilities and develop migration plans to meet developed architectures and standards.

- RECOMMENDATION: The IC should be fully compliant with the standards of emerging U.S. communications systems whenever and wherever possible, to ensure required data movement.

- RECOMMENDATION: The IC should invest to ensure that its system for collection, processing and analysis can access a communications point for dissemination.

- RECOMMENDATION: The IC must also invest to ensure the capability to service unique communications requirements that cannot be satisfied by the communications community. An example of this would be support for clandestine communications.

- RECOMMENDATION: The communications infrastructure supporting intelligence dissemination must move to support a "virtual worldwide architecture."

- **RECOMMENDATION: The IC must do a better job of putting intelligence into a form that is usable with the users' systems.**

- **RECOMMENDATION: The Secretary of Defense should exercise his authority to create a separate Assistant Secretary of Defense for Intelligence, reporting directly to the Deputy Secretary of Defense.**

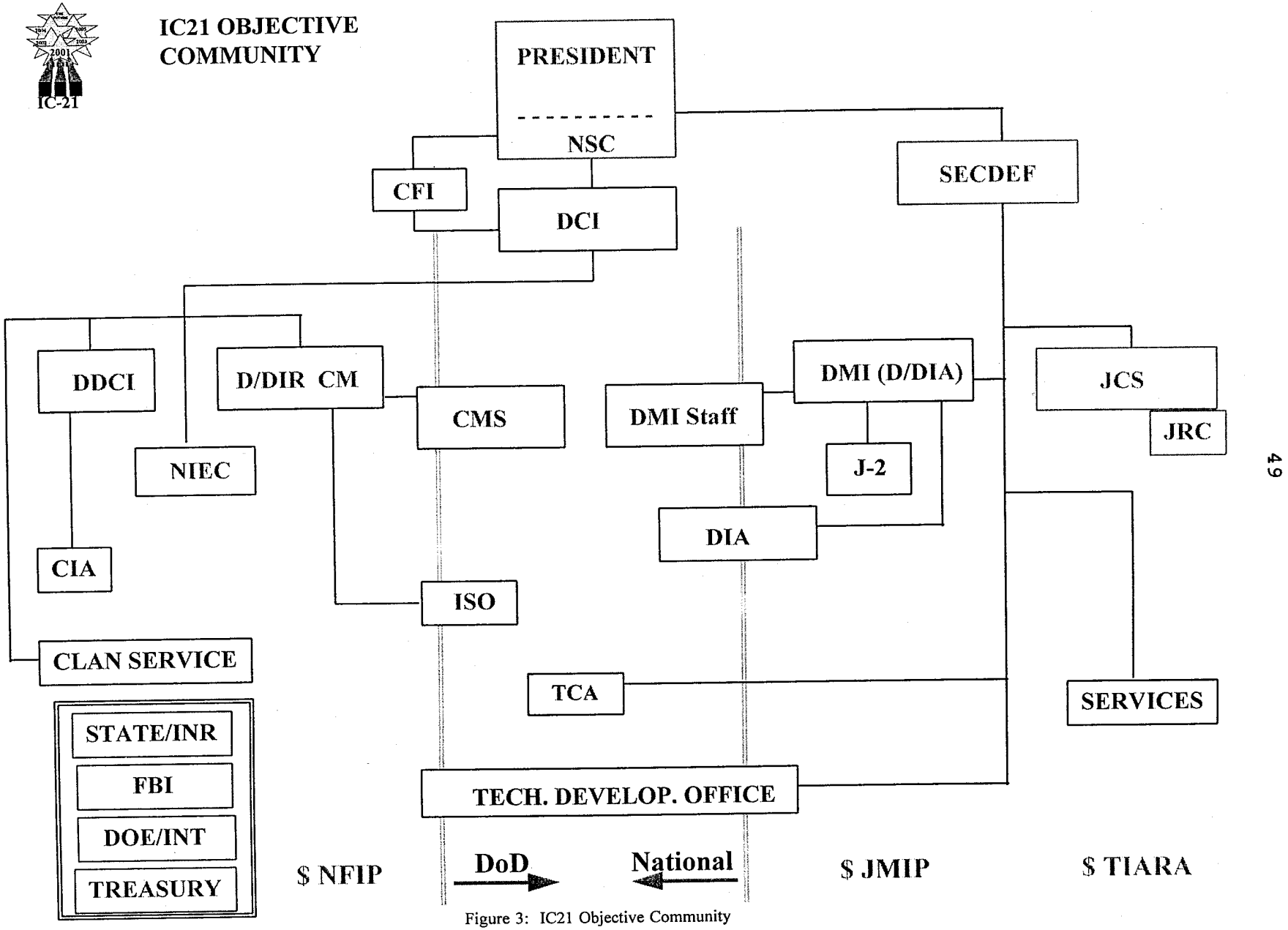

Figure 3: IC21 Objective Community

IC FUNCTIONS

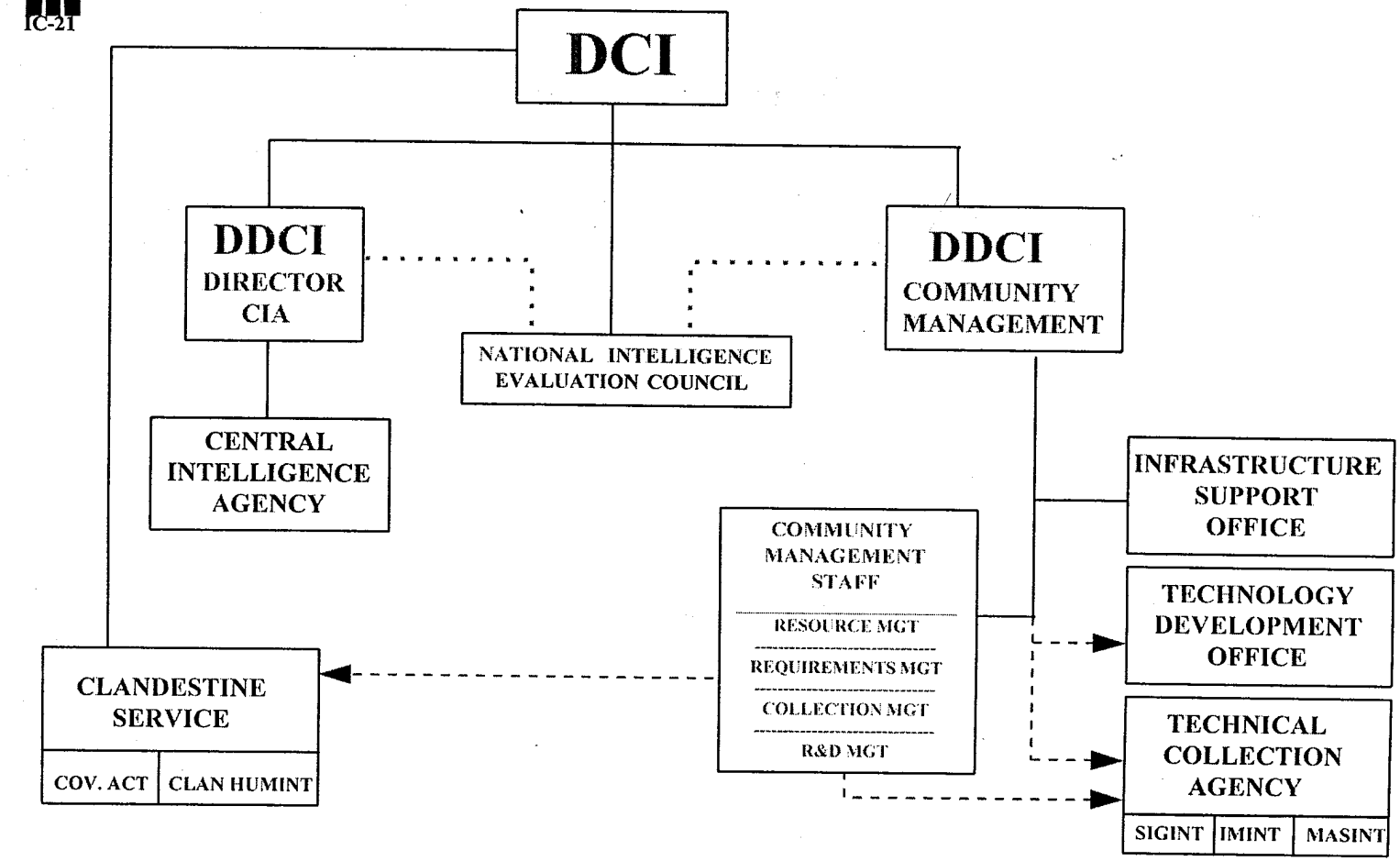

Figure 4: IC Functions

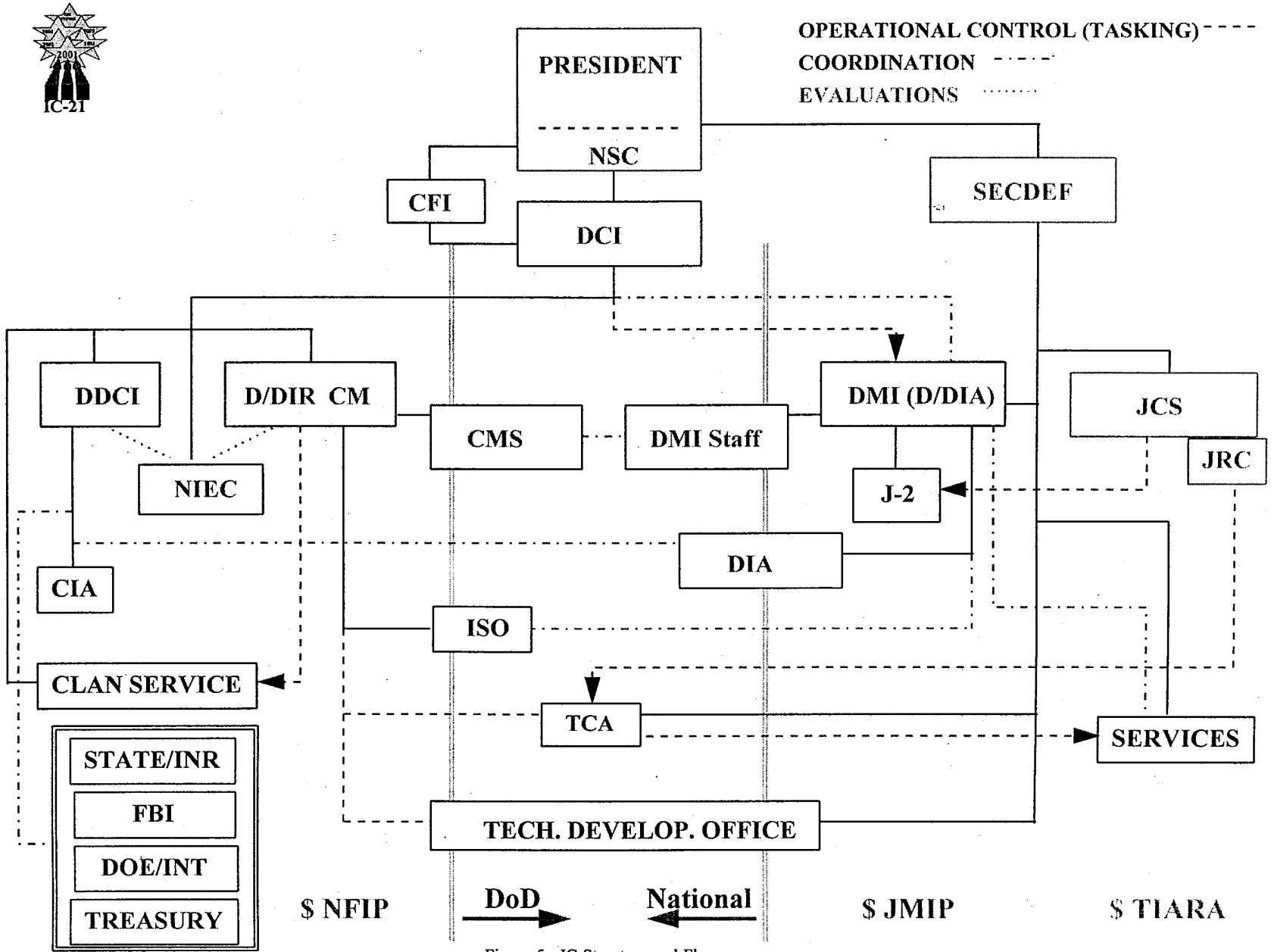

Figure 5: IC Structure and Flow

INTELLIGENCE COMMUNITY MANAGEMENT

Executive Summary

One of the centerpieces of the *Intelligence Community for the 21st Century (IC21)* review is a hard look at Intelligence Community (IC) management and the development of a proposed community model that synthesizes the findings and recommendations of the other staff studies. At the beginning of this undertaking, a hypothesis was developed that the IC and its customers would benefit, either through performance enhancement or cost reduction or both, from a more corporate approach to intelligence. This hypothesis was then "tested" in the following specific areas: planning, programming and budgeting; collection management; production management; personnel management; and research and development. The goal was to identify what specifically would improve management of these areas, and whether or not a more corporate approach would be constructive. Then, if a more corporate approach were dictated, to identify what changes in organization, function, and authority would be required to achieve it.

Perhaps not surprisingly, we discovered that the Intelligence Community would benefit from a more corporate approach in each of the major areas we addressed. In order to form a flexible "tool kit" of capabilities for the future, the Director of Central Intelligence (DCI) and his staff require additional authorities and different management structures to create a unified, effective and efficient community. Services of common concern should be consolidated at the community level. Programming and budgeting and personnel management must be more centrally managed. Collection must be managed coherently across the disciplines, with increasingly difficult resource trades made at the community level in an informed, all-source process. Improved synergy during collection operations, which will become more and more critical to success in the 21st century, requires movement away from the traditional stovepipe approach to collection. Research and Development requires closer coordination with requirements, and a contingency fund for "good ideas" should be established to allow the community to take advantage of technological targets of opportunity.

The community needs to become a corporate entity; personnel reform that promotes lateral movement among agencies and a community SES cadre is essential. The primacy of all-source analysis needs to be reinforced, and strong links forged between analysts and policy-makers and analysts and collectors. The community should be, and to an extent already is, moving toward a "virtual analytical environment" that requires a new set of skills and management techniques. Increased centralization of management functions must be balanced by a strengthened and independent evaluative function.

Clandestine operations will continue to be both the riskiest and potentially the highest-payoff intelligence operations, becoming increasingly important in the 21st century due to the likely nature of future targets. This aspect of the intelligence community requires a more intensive level of management involvement on the part of the DCI and should be housed in a separate organization, with a direct reporting chain to the DCI.

The defense intelligence community also stands to benefit from more coherent and centralized management. A Director of Military Intelligence with enhanced control over defense intelligence programs and operations would serve as both a senior military advisor to the Secretary of Defense for intelligence, and a locus for the close coordination required between the national and tactical intelligence communities and budgets.

INTELLIGENCE COMMUNITY MANAGEMENT

I. Approach

One of the centerpieces of *The Intelligence Community in the 21st Century (IC21)* review is a hard look at Intelligence Community (IC) management and the development of a proposed community model that synthesizes the findings and recommendations of the other staff studies. At the beginning of this undertaking, a hypothesis was developed that the IC and its customers would benefit, either through performance enhancement or cost reduction or both, from a more corporate approach to intelligence. This hypothesis was then "tested" in the following specific areas: planning, programming and budgeting; collection management; production management; personnel management; and research and development. The goal was to identify what specifically would improve management of these areas, and whether or not a more corporate approach would be constructive. Then, if a more corporate approach were dictated, to identify what changes in organization, function, and authority would be required to achieve it. Although they are presented first in this document, the role and authorities of the Director of Central Intelligence (DCI) were considered last, in the context of the needed changes in the above-mentioned areas.

II. Introduction/Assumptions

It immediately became clear that it is impossible to measure the effectiveness of something without a standard by which to measure -- an understanding of the purpose and role of intelligence, and its appropriate relationship to policy and national strategy. With very little research it became apparent that there has historically been disagreement on these topics, and that the level of disagreement is greater today, in the post-Cold War period, than it has been for some time. This makes it necessary to examine these issues in at least a cursory way in order to establish some assumptions without which the answers to the questions posed by this study would be meaningless.

At the most basic level, there have been, and remain, two diverging views of the appropriate role of intelligence in the United States. One view maintains that intelligence provides impartial and objective information to policy-makers; intelligence is a truth-seeking profession and the policy community is a customer who does not and should not influence the product. The other, and less widely held, view is that intelligence is in fact an instrument of policy and should be used to both shape and further policy goals: the intelligence and policy communities must act as partners. The

question of whether intelligence informs policy or serves it is truly a chicken-or-the-egg issue -- we believe it must do both at different times. Tending too far in either of these directions threatens lack of relevance on the one hand, and politicization on the other. The challenge for the IC is to maintain a balance of objectivity and involvement, a goal that can only be met with the cooperation and understanding of the policy community. This study assumes that the basic structure of the United States government, including its policy apparatus, will remain relatively stable at the departmental level, but that the policy community may be influenced positively by recommended changes in its formal relationship to the IC.

Another basic question that must be raised is that of the evolving definition of national security. Although there may be a consensus that intelligence exists primarily to identify potential threats to the national security of the United States, the definition of those threats, and perhaps the threats themselves, change over time. We have seen an evolution from nation-based threats and conflicts to trans-national threats and regional and ethnic strife. New areas of intelligence emphasis, such as proliferation and terrorism, clearly represent emergent threats to our national security. Other, less clear-cut areas of endeavor, such as economic and environmental intelligence, remain subjects of debate concerning the closeness of their relationship with national security, how much value intelligence actually adds to these areas, and at what cost to other, higher priorities. Regardless, all of these areas of endeavor represent a new level of complexity for the IC, requiring an "interdisciplinary" approach to intelligence and a different set of skills than that needed in the Cold War world.

Each Administration will be faced with defining threats to national security, and the results will vary. In the absence of definitive guidance, the IC will inevitably try to be all things to all people. Therefore, it is a mistake to structure the community to meet currently articulated or even projected future threats except in the most general sense. In looking to the 21st century, it is important to reach a consensus on the core missions and capabilities of the IC, and to add to those missions only on a pay-as-you-go basis. The new approach to mission-based budgeting, which creates four primary mission areas (support to policy makers, support to military operations, support to law enforcement, and counterintelligence), and within those areas identifies core capabilities, sustaining capabilities and supporting capabilities, appears to be a move in the right direction. The community of the future should be based on the capability and flexibility to perform those basic functions -- a "tool kit," if you will, for the challenges of the next millennium.

Within the IC, there are a series of checks and balances. Starting at the top, the relationship between the DCI and the Secretary of Defense (SECDEF) epitomizes an important tension in the community: support to military operations (SMO) versus support to national-level policy makers. Considering that military operations are an instrument of policy, SMO is in fact another facet of support to the policy-maker, but it is of a different and potentially all-consuming sort. The Department of Defense

(DoD) is the largest customer of intelligence information, and that justifies its significant voice in the process; the DCI, however, must be able to protect the equities of the civilian policy-makers and the longer-term interests of the nation (a more detailed discussion of this tension is contained in both the *Intelligence Support to Military Operations* and the *Intelligence Community Surge Capability* staff studies). That much of the intelligence community is a shared resource is at times problematic, but is in accord with statutory direction to "eliminate waste and unnecessary duplication within the intelligence community." It makes sense from a resource perspective, as long as appropriate management safeguards exist to ensure that no customer's needs are shortchanged in the process.

Another balance issue within the community is the role of the program manager vis-a-vis the issue coordinator. The Needs Process has established an increasing tension between the issue coordinators, who are looking across programs to fund priority activities that contribute to their individual areas of responsibility adequately, and the program managers, who are faced with satisfying the requirements of all of the issue managers and must make internal trades to build a coherent and sustainable program. This would be more of a contest if the issue coordinators had any real leverage over the budget process, but currently they do not. A similar case is the lesser, but still important, tension between functional managers and program managers. Because the program managers build the budget, and the issue coordinators and functional managers can basically only advise and recommend, the balance of power is skewed in favor of the program managers. In any scheme of intelligence community management, there will be competing requirements of this type. The challenge is to create a programming and budgeting process that minimizes destructive competition and can adjudicate competing requirements and priorities in a balanced way.

Finally, the Congressional intelligence oversight function, unique to this nation, represents one of the legislative checks on the executive branch that is the hallmark of our system of government. The two intelligence committees, in turn, provide a check on each other in the performance of this function. Although this makes for a complex and sometimes inefficient system, in the long run it protects the interests of the American people. Within the IC as within the government at large, some of these existing balances may need to be recalibrated; overall, however, they serve a useful purpose and should not be lightly set aside.

III. Summary of Findings:

Perhaps not surprisingly, we discovered that the IC would benefit from a more corporate approach in each of the major areas we addressed. In order to form a flexible "tool kit" of capabilities for the future, the DCI and his staff require additional authorities and different management structures to create a unified, effective and efficient community. Services of common concern should be consolidated at the

community level. Programming and budgeting and personnel management must be more centrally managed. Requirements and collection must be managed coherently across the disciplines, with increasingly difficult resource trades made at the community level in an informed, all-source process. Improved synergy during collection operations, which will become more and more critical to success in the 21st century, requires movement away from the traditional stovepipe approach to collection. Research and Development (R&D) needs to be more closely coordinated with requirements and a contingency fund should be established to take advantage of technological targets of opportunity.

The community needs to become a corporate entity; personnel reform which promotes lateral movement among agencies and a community SES cadre is essential. The primacy of all-source analysis needs to be reinforced, and strong links forged between analysts and policy-makers and analysts and collectors. The community should be, and to an extent already is, moving toward a "virtual analytical environment" that requires a new set of skills and management techniques. Increased centralization of management functions must be balanced by a strengthened and independent evaluative function.

Clandestine operations will continue to be both the riskiest and potentially the highest-payoff intelligence operations, becoming increasingly important in the 21st century due to the likely nature of future targets. This aspect of the IC requires a more intensive level of management involvement on the part of the DCI and should be housed in a separate organization, with a direct reporting chain to the DCI.

The defense intelligence community also stands to benefit from more coherent and centralized management. A Director of Military Intelligence (DMI) with enhanced control over defense intelligence programs and operations would serve as both a senior military advisor to the SECDEF for intelligence, and as a locus for the close coordination required between the national and tactical intelligence communities and budgets.

IV. Roles, Relationships and Authorities

Role of the DCI

The role and authorities of the DCI are central to achieving the goal of a more corporate IC. There are two broad areas at issue: (1) the role of the DCI vis-a-vis the President; and (2) the role of the DCI within the IC.

Several witnesses, including several past DCIs and Deputy DCIs, noted that the degree to which the DCI visibly commands the respect and confidence of the President is central to the DCI's effectiveness. Realistically, however, there is no way to mandate or to legislate a close working relationship between these two officials.

Two suggestions repeatedly surface regarding the status of the DCI. The first is that he be made a cabinet-rank official. The second is that he be given a fixed term of office. The study group does not believe that either of these has sufficient merit or would achieve the goal of a stronger DCI. The third is that he be relieved of his responsibilities for the Central Intelligence Agency (CIA) and elevated to a position over the entire IC.

Cabinet-rank for officials who are not members of the Cabinet (*i.e.*, the heads of departments) is merely an honorific. The United States does not have Cabinet government; being designated a member of the Cabinet does not in any real sense increase one's authority. It certainly will not enhance or improve the DCI's relationship with the President, which can only be based on an existing level of trust and confidence. Indeed, mandating Cabinet-rank for the DCI while doing anything less than creating a true Intelligence Department -- which no one has contemplated -- only calls more attention to the disparity between the DCI's responsibilities and his authority, even with the enhancements being proposed here.

The importance of the DCI's personal relationship with the President is also the main argument against a fixed term. Proponents of a fixed term argue that this would have several benefits. Ten years is often suggested, as has been done with the Director of the Federal Bureau of Investigation (FBI). First, and perhaps foremost, a fixed term would provide for greater continuity and stability than we now have. Until 1977, it was not customary for the DCI to be replaced with a new administration. That is no longer the case. Moreover, the DCI's position has since been subjected to fairly frequent turn-overs over and above presidential transitions. From 1973-1977 there were five DCIs; from 1991-1996 there have been four DCIs. However, a fixed term could create the situation where a President would inherit a DCI with whom he could not work. Although there would be greater continuity, the DCI's effectiveness would diminish rapidly, a far greater loss. As noted, an analogy is often drawn to the Director of the FBI. The comparison is inapt. The DCI is the chief intelligence officer and deals directly with the President. The Director of the FBI is not the chief law enforcement officer; the Attorney General is and serves at the President's pleasure. In sum, a fixed term would not be an improvement.

The National Security Act states that the DCI is the head of the IC and the President's principal intelligence adviser. Neither of these designations for the DCI is the same as meaningful control. If the IC is to achieve a greater degree of coherence and corporate identity, then the role of the DCI has to be changed. The glaring gap between his responsibilities and his authorities has to be closed to the greatest extent possible. The DCI should be viewed as a chief executive officer of the IC, with purview over all of its major functions and a greater degree of control over budgets, resources and major policy issues that are common to all agencies. However, the testimony of former DCIs and other former senior IC officials all concur that the DCI

needs an agency "of his own" -- *i.e.*, the CIA -- if he is to have any real power within the IC.

The National Security Council

The National Security Act also places the DCI under the direction of the National Security Council (NSC). The NSC is composed of four officials: the President, the Vice President, and the Secretaries of State and Defense. The IC is a service organization. It has no meaning without its relationship to policy makers. Thus, the DCI must have regular contact with the NSC members. However, it is not reasonable to expect that they can give the DCI and, through him, the IC, the kind of regular executive guidance that was envisioned by the National Security Act. Indeed, in each successive Administration, there has been some sort of sub-NSC group created to deal with intelligence, reflecting the shortcomings of the NSC itself to carry out this role.

Finally, many witnesses at hearings and staff panels and the oversight experience of this Committee indicate that certain intelligence activities -- clandestine operations and covert action -- require special attention. These activities consume an inordinate amount of the DCI's time, in terms of both management and testimony before Congress. In the future, certain types of offensive information warfare (IW) activities conducted in peacetime or outside the context of a military operation may also fall into this category. We do not question the utility of these activities and believe that the United States must have recourse to them. At the same time, executive control can and should be made more direct. It is important for the DCI to maintain close control over these activities.

The following recommendations are designed to resolve the issues noted above. Beginning with the issue of executive guidance, of the various sub-NSC bodies created to deal with intelligence, the Committee on Foreign Intelligence (CFI) created by President Ford in 1976 appeared to be among the more successful, in terms of its stated role, its membership and its performance. Interestingly, the Senate Select Committee on Intelligence proposed re-establishing this group in legislation in 1992, as has the Aspin-Brown Commission. We believe that the CFI, properly constituted and empowered, can more usefully serve as a body to provide the DCI and the IC with the necessary guidance and policy-maker oversight. This is not meant to supplant the DCI's current direct access to the NSC members; it is meant to give the DCI access on a more regular basis to senior policy-makers who can give direction to the IC and can listen to and relay IC concerns.

Two Deputy Directors of Central Intelligence

As noted, we do not find major flaws in the broader parameters of the role of the DCI as currently described in legislation in terms of his tenure or his responsibility for the CIA. The DCI should continue to serve at the pleasure of the President and

continue to exercise control over the CIA and the Community Management Staff (CMS), and have direct control over the Clandestine Service. The DCI would, thus, continue to have multiple major responsibilities. All DCIs have found this a broad and sometimes difficult mandate. The ability to delegate is important, although it has been done differently by virtually every DCI. The current DCI, for example, relies on two executive directors -- one for the CIA and one for the CMS. Their titles belie their responsibilities. The positions responsible for these two large parts of the DCI's portfolio should be enhanced and their duties better defined. Given the importance of their positions, Senate confirmation also appears necessary. Some permanence in the DCI's supporting structure is needed and can be achieved without losing necessary flexibility. It also allows for greater institutional continuity, clearer definition of responsibilities and improved congressional oversight.

In order to minimize superfluous bureaucratic layering, we concluded that the current position of Deputy DCI (DDCI) should specifically be given day-to-day responsibility for the CIA, whose enhanced analytical responsibilities are discussed below. This would reduce layering, would continue to give the DCI direct access to his major bureaucratic and institutional base, and yet would relieve the DCI of many lesser administrative concerns. Paralleling this first DDCI, there should be a second DDCI for Community Management, for much the same reasons, with purview over the collection, acquisition and infrastructure elements of the IC. There are also changes in the DCI's budget and personnel authorities, noted below. As currently allowed by law, either the DCI or one of his DDCIs -- but no more than one -- could be a military officer. The DCI would select which of the DDCIs would act as DCI in his absence.

As noted above, the importance of the DCI's relationship with the President is such that few prerequisites for nominees should be imposed. However, to the extent possible, these DDCI positions should be considered as professional as well as political appointments and should go to individuals with extensive national security or intelligence background. This is especially important if a DCI with less such background is chosen. The two DDCIs should be confirmed by the Senate, just as is the current DDCI position.

The Central Intelligence Agency

The CIA, which would now be directed by the DDCI, was envisioned by President Truman as a coordinator of disparate intelligence being produced by other agencies. The CIA quickly became a producer in its own right because of policy-maker demands, the unwillingness of then-existent agencies to respond, and an aggressive CIA leadership. Although this is different than President Truman's vision, we do not believe that this development should be reversed. Indeed, it would appear more profitable to underscore the CIA's analytical role by confirming it as the premier all-source (*i.e.*, deriving its analysis from all intelligence collection disciplines) analytical agency within the IC.

We concur with the observation of former DCI Richard Helms that the President needs his own analytical group and that if we did not have the CIA today we would probably invent it. Underscoring this role means more than words. The CIA should house not only its analysts, but the second- and third-tier exploiters of the various intelligence collection disciplines. By bringing them closer together we can improve the efficiency of the all-source analytical process and achieve a true synergy between collection and analytical production.

The Clandestine Service

Given the political and administrative problems raised by clandestine operations and covert action, their bureaucratic tie to the DCI must be made more direct. At present as many as two or three officials are between the DCI and the CIA's Directorate of Operations (DO). Moreover, there is no compelling substantive reason for the DO to be part of the same agency as the analytic Directorate of Intelligence (DI). This is largely the product of historical accident and the bureaucratic aggressiveness of DCI Walter Bedell Smith, who expanded CIA activities into both operations and analysis in the early 1950s, when other agencies failed to meet policy-maker needs in these areas.

We believe that it would be better for the DO, renamed the Clandestine Service, to be a distinct entity, under the direct control of the DCI. This would rationalize the structure of the CIA as the premier all-source analytical agency. The Clandestine Service and the CIA can continue to be housed in the same building. However, both the Clandestine Service and the CIA could also be managed more effectively if they each had one major task. The separation of the Clandestine Service should also reinforce the fact that clandestine Human Intelligence (HUMINT) serves the entire community and not just the CIA. The Clandestine Service would conduct all clandestine HUMINT operations, even those undertaken by military personnel, who would be integrated into the organization.

There should be a Director of the Clandestine Service, reporting directly to the DCI. This individual should be an intelligence professional. After much debate, we recommend that this individual not be subject to confirmation by the Senate. The sensitivity of this position is such that the DCI must be free to choose the man or woman upon whom the utmost reliance can be placed. Senate confirmation raises a number of other political considerations that might best be avoided. This recommendation, coupled with the role of the new DDCI/Community Management, should also allow a closer integration of collection management and operations, and should enhance oversight of clandestine operations. The Director should have a deputy who is a two-star active duty military officer (further details are contained in the *Clandestine Service* staff study).

NFIP Defense Agencies

If the IC is going to achieve the goal of "corporateness," and if the DCI is going to function as a true CEO, then he should have a greater say in the selection of his "corporate team" -- the heads of the other major intelligence components. Current law requires that the SECDEF "consult" with the DCI in naming heads for National Foreign Intelligence Program (NFIP) defense agencies. Although it is unlikely that the SECDEF would nominate someone to whom the DCI is strongly opposed, it is possible. Instead, the DCI's advice and *concurrence* should be sought. In the unlikely event of disagreement, the issue could be referred to the NSC Committee on Foreign Intelligence or, ultimately, to the President. But the importance of a truly corporate team requires a stronger DCI voice in this process. The study group believes, however, that the role of the NFIP defense agencies is so substantially different from that of the other departmental elements of the NFIP that this arrangement is not appropriate for the State, Energy or Justice Departments. The defense agencies are primary collectors and producers of intelligence without whom the DCI could not perform his statutory functions, while the other departmental elements are analytical efforts focused on tailoring intelligence products for their departmental consumers. Therefore, we recommend no change in the selection process for those activities.

Director of Military Intelligence

The Defense Department -- civilian policy makers and military services at all levels -- is one of the largest components and mostly important customers of the IC. Many of the larger organizational issues noted for the IC at large are also found within the defense-related part of the IC. Enhancing the DCI's authority solves some, but not all, of the problems. It is important that the defense intelligence establishment also have a single, uniformed official who is both responsible for and empowered to address these issues, or to advise the SECDEF about them. We believe that this should be a three-star military officer, carrying the title of Director of Military Intelligence (DMI). The study group also believes that this individual should be dual-hatted as the Director of the Defense Intelligence Agency (DIA), the program manager of the Joint Military Intelligence Program (JMIP), and program coordinator for the Tactical Intelligence and Related Activities (TIARA). Although previous proposals for a DMI have sought a four-star office, the study group believes a four-star officer is neither appropriate nor likely to be approved. For the senior military intelligence officer to be on a par with the Chairman of the Joint Chiefs of Staff (CJCS) and the Commander in Chief is not appropriate for a supporting function such as intelligence, and could potentially promote an unhealthy rivalry between the DMI and the DCI, particularly if the DCI were to remain as currently constituted, i.e., not of cabinet rank. The DMI would report to the DCI on IC-wide issues and activities.

The three-star DMI concept consolidates management of defense intelligence across the NFIP (DIA), JMIP and TIARA and continues to provide intelligence support

to both OSD and CJCS, via the J-2, and a unified J-2/DIA staff. The DMI would not control the DoD agencies within the NFIP, but would be responsible, as currently, for all defense analysis, production, and overt HUMINT operations. As program manager for JMIP, the DMI would ensure a coherent program that complemented national and tactical capabilities. As program coordinator for TIARA, he would ensure that the services' intelligence programs were interoperable and consistent with the larger intelligence architecture. The DMI would need a significantly enhanced staff element to handle program and budget activities for the JMIP and TIARA formerly handled by the office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I)), and to be responsible for defense intelligence architectures and coordination with the community systems and architectures office.

Assistant Secretary of Defense for Intelligence

The position of ASD (C3I) is, in the study group's view, an artificial construct. Although C3I for the Warrior and related concepts have been constructive in encouraging the Services and DoD to integrate intelligence and information handling techniques better into Command, Control and Communications (C3) architectures, integration of C3 and Intelligence as staff functions has simply not happened, either in ASD(C3I) or in the Joint Chiefs of Staff (JCS). One can also make an argument that in the Information Age, intelligence needs to become increasingly linked to operations; C4I for the Warrior may support this operational concept in theory, but is of limited utility for staff planning purposes. To date, most, if not all, Assistant Secretaries for C3I have placed primary emphasis on the "C3" rather than the "I." Similar emphasis must be placed on intelligence if doctrinal concepts such as Dominant Battlefield Awareness are to be realized. One aspect of this increased emphasis is a more corporate approach to intelligence as embodied by a DMI. The other aspect is a stronger policy presence in Defense. Consequently, the study group believes that defense intelligence would be better served by having a separate Assistant Secretary of Defense for Intelligence (ASD(I)), an option that the SECDEF could exercise at any time. Regardless, the role of the ASD(C3I) or ASD(I) should be policy, planning and oversight; the programmatic and budgeting functions that have devolved to ASD(C3I) should be handled by the DMI staff.

Infrastructure Management

Numerous studies and reviews of the community, including the National Performance Review, have concluded that there are efficiencies and potential cost-savings to be had by consolidating infrastructure and "services of common concern." During the course of this study, it became apparent that it makes sense to combine under centralized management, although not necessarily in one place, such community functions as personnel management, security, certain types of training,

communications, and automation.[1] Although many of the personnel performing these functions could remain physically in place as support detachments, the study group believes that an Infrastructure Support Office should be established to manage these areas across the community. The growth of the IC and proliferation of distinct agencies have led to unwarranted duplication in what are, essentially, administrative and logistical functions. This is not only duplicative and costly, but also can harm the ability of the IC to operate as a corporate whole.

Finally, these recommendations raise one final question about oversight. There is, currently, a statutory Inspector General (IG) for the CIA and for DoD. In order to ensure that major IC-wide functions are available to necessary scrutiny, the current CIA IG should serve as the IC IG, operating, when necessary, in conjunction with the DoD IG for NFIP Defense agencies.

Recommendations:

1) **Reestablish the Committee on Foreign Intelligence to provide the DCI with necessary guidance and feedback. The Assistant to the President for National Security should chair the CFI; other members should be the Secretaries of State and Defense, the Chairman of the JCS, and the Attorney General, or their deputies.**

2) **Create two Deputy Directors of Central Intelligence: a DDCI to manage the CIA, responsible for all IC production and analysis; and a DDCI for Community Management, responsible for requirements, collection and resource management. Both DDCIs should have extensive national security experience; both should be confirmed by the Senate. At no time should more than one of the three (DCI and two DDCIs) be active duty military. The DCI will designate one of the DDCIs to serve as the acting DCI in his absence.**

3) **Designate the Director of DIA as the Director of Military Intelligence (DMI). The DMI will be the program manager for the JMIP and the program coordinator for TIARA.**

---

[1] The INFOSEC function, that is currently a non-NFIP MFP III program, could also be managed by this consolidated activity in better cooperation with communications and ADP; it could remain at physically at NSA or the TCA, as later discussed, to continue to enjoy the synergy between the "makers and the breakers" of codes, but would respond to community direction. Funding could be split between JMIP and TIARA, and management coordinated with the DMI staff and DMI.

4) **Increase the DCI's role in the appointment of NFIP agency directors by requiring the Secretary of Defense to obtain his "advice and concurrence" for these appointments.**

5) **Urge the Secretary of Defense to consider creating an Assistant Secretary of Defense for Intelligence.**

6) **Create a separate Clandestine Service directly accountable to the DCI. The Director of the Clandestine Service should be selected by the DCI from among intelligence professionals. The Deputy Director should be a two-star military intelligence officer.**

7) **Create an Infrastructure Support Office (ISO) which consolidates services of common concern across the community, to include at a minimum personnel, security, training, communications and automation.**

V. Collection and Requirements Management

One of the IC's main shortcomings is an inability to manage collection optimally across disciplines or "INTs." This shortcoming is reflected in two areas: in short-term collection management against current intelligence problems, and, more seriously, in longer-term resource reallocation between collection disciplines based on an examination of intelligence needs, the most appropriate mix of collection assets to fulfill those needs, and an evaluation of how well those assets perform against their tasking. Collection requirements and tasking are currently handled by committees that make resource and tasking decisions in a single-source context that does not promote an optimal all-source approach to collection problems. In the global and resource environment envisioned for the future, competition for collection assets, already stiff, will only increase. Trans-national problems such as proliferation require integrated, all-source solutions. With the collapse of the Soviet Union, even as more information becomes available from open sources, the remaining "hard" targets have become tougher to crack, also necessitating a coordinated, multi-INT approach. The tension between military requirements -- now expanded to include humanitarian and peacekeeping missions -- and longer-term national interests will become greater and the mechanism for making decisions such as whether or not to move a satellite from one region to another must become more robust. The IC needs a management staff with the resources and authorities to build and maintain a coordinated collection program, and keep it in balance with the production and infrastructure elements of the community.

What community management is currently provided comes from the National Intelligence Collection Board, a companion organization to the National Intelligence Producer's Board. Although this forum is beginning to become more "energized" under its new chief, it is not yet the body to compel the needed integration of the

collection process within the community. The fact that the Executive Director (ExDir) for Community Affairs and the Associate Director of Intelligence for Military Affairs are planning the establishment of a Collection Operations Management Group indicates an awareness of this problem. This organization, or something like it, needs to exist at the community level, with representatives from the programs and DoD/JCS, to provide an integrated forum for collection decisions and to mediate conflicts between short-term military and longer-term policy-maker support. This organization could either supersede or be superimposed upon the current entities involved in single-INT tasking: COMIREX, the Signals Intelligence (SIGINT) Committee, the Measures and Signatures Intelligence (MASINT) Committee, and the National HUMINT Requirements and Tasking Center.

For short-term collection against current intelligence targets, there are two collection management centers within the Community, one at the CIA and one at DIA. Although these centers can be said to work reasonably well, the coordination mechanism between them is not well-defined. Also, tasking collection or requesting information within the current system is inefficient. At some point in the requirements chain, a customer with a requirement must submit a SIGINT or Imagery Intelligence (IMINT) collection request, rather than a general request for information. It is virtually impossible for a requestor to ascertain whether the information he requires has already been collected and exists in a database somewhere or must result in new collection tasking. The IC needs a system that centrally manages information requests, and a focal point for managing this process across the community. Although some progress has been made towards this goal, it has been done mostly on an "INT by INT" basis rather than as a community-wide, all-source effort. However, the Intelligence Systems Board (ISB) has proposed a Request For Information (RFI) management system that would further this goal.

One cannot discuss collection without addressing "stovepipes." To illustrate the long-standing nature of this debate, the following is a quote from Community Management Task Force Report commissioned by then-DCI Robert Gates and conducted by Danny Childs and Rich Haver in 1991: "We have made one key assumption -- that vertical collection management structures are created. We should note, however, that there is a body of opinion that strongly doubts the wisdom of creating such 'stovepipes.' One concern is that powerful checks and balances will be needed to compensate for the possible tendencies of such strong functional managers to operate unilaterally and make decisions with an eye to resource advantage. A second concern is the possibility that community requirements will not be equitably addressed without the aid of a strong independent body as a requirements authority."

Although the existence of stovepipes was an assumption for that report, the study group believes that it is no longer wise or even possible to accept stovepipes as a given. There are real benefits to be achieved by creating a more unified management structure for technical collection operations. MASINT, in particular,

which many view as the "INT of the future" because of its potential application for some of the more difficult intelligence problems such as proliferation, would benefit from an approach that does not view it as a competitor to SIGINT and IMINT, but rather as a complementary discipline making use of many of the same sources of collection (see the *MASINT : Measurement and Signatures Intelligence* staff study for more details). As noted above, the key to future success against difficult collection problems with shorter and shorter timelines is to achieve greater synergy between the collection disciplines. Wherever this occurs, the results are greater than the sum of the parts. Instead of designing cumbersome systems "after the fact" to tip off collection assets operating within a completely different conceptual and operational framework, these operations need to be conceptually integrated from the beginning and managed coherently. The target environment itself is beginning to blur the lines between the technical disciplines.

The truth is that, to a certain extent, stovepipes are unavoidable; the issues are how far up they extend and whether or not a mechanism exists to ensure interaction between them at the operational level. Although the technical collection disciplines share many elements (as several interviewees told us, "it's all about bandwidth") and will undoubtedly become increasingly similar in the future, there are nevertheless distinct skills and training requirements associated with SIGINT, IMINT and MASINT -- and HUMINT collection is significantly different from all the others. Although the study group believes that all of the technical disciplines would benefit from being managed in a coherent fashion, the different endeavors are not, in the foreseeable future, interchangeable, and it is important to maintain the levels of expertise in each of these areas that have contributed to our success to date. Therefore, if the technical collection disciplines were combined into one agency, as we recommend, there would in all likelihood be "mini-stovepipes" within it. This would not necessarily be a bad thing as long as there was cross-leveling activity both at the operator level and at the top, where it would all "come together" under the control of one individual. Under a consolidated collection concept, technical control of the various collection disciplines would be vested in the director of the collection agency and delegated to designated functional managers for each discipline. The director of the collection agency would thus assume the Director of the National Security Agency 's (NSA's) responsibilities as SIGINT advisor to both the DCI and the SECDEF, and perform similar functions for IMINT and MASINT.

Additionally, the best collection operations occur when collectors and analysts work closely together, so it is important to keep the "first-line" analysts or exploiters with the collectors. These analysts provide immediate feedback to the collectors, report on time-perishable information, and act as a "bridge" to the all-source analytical community, with whom they should be electronically linked. Although we acknowledge that the dividing line between first-line exploiters and second- and third-tier analysts is not as clear-cut in the SIGINT arena as it is in the imagery world, we nevertheless believe it is possible to distinguish between these levels of analysis in a

systematic way (see the *SIGINT: Signals Intelligence* staff study for more details). It is equally important to leave first-tier HUMINT exploiters such as reports officers with the HUMINT collectors.

Although the technical collection disciplines could reasonably and effectively be combined into one agency, it is the opinion of the study group that HUMINT collection can and should remain apart, with overt HUMINT collection continuing to be conducted by DIA and the State Department, and all clandestine HUMINT collection operations falling under the purview of the Clandestine Service (see the *Clandestine Service's* staff study for more details on this concept). HUMINT tasking and operations are different enough that there is little to be gained by combining its management with that of the technical collection disciplines, and, as mentioned earlier, its risks are such that it warrants a more intensive level of organizational oversight. There are, however, numerous instances where HUMINT supports technical collection in extremely important ways. To maintain effective cooperation in these areas, an aggressive rotation policy is required to ensure that clandestine operations personnel are employed in the collection areas supported by their efforts, and that technical personnel are employed where they can affect the tasking of HUMINT assets. It is also important to note that clandestine HUMINT collection tasking and requirements, along with all other collection operations, will be managed by the CMS and reviewed by the National Intelligence Evaluations Council (NIEC). (The NIEC is discussed in the *Intelligence Requirements Process* staff study.

The study group also considered whether or not it was advantageous to combine Open Source collection with the technical collection disciplines. Although clearly areas of similarity exist, we determined there was little to be gained from this proposal. Since the primary focus of Open Source collection is the management of huge amounts of information that are readily available rather than the attempt to collect information from denied areas or that the originator does not wish anyone to have, it was decided to place responsibility for Open Source with the analytical agencies, primarily the CIA.

Recommendations:

1) **Create a community-level requirements and collection management activity within the CMS responsible for directing collection tasking to the appropriate organizations and ensuring a coherent, multi-INT approach to collection problems.**

2) **Create and centrally administer a community-wide system for RFI management.**

3) **Create a Technical Collection Agency (TCA) that combines SIGINT, IMINT and MASINT collection, processing and first-tier exploitation and analysis. The TCA should be a Type 3 Combat Support Agency, and its director should be either a senior defense or intelligence civilian or a flag officer.**

VI. Production Management

There are three primary, sanctioned producers of all-source intelligence products in the IC: the CIA, DIA, the State Department's Bureau of Intelligence and Research (the Department of Energy's Intelligence Division is also an all-source producer of tailored products for its departmental consumers). Although the appropriateness of the State Department maintaining its own analytical capability is rarely questioned, many have suggested that the separate DIA and CIA efforts are not necessary. However, in our view, reality dictates that the Defense community must have its own analysis and reporting capability. If we were to do away with DIA, it would be recreated in another form somewhere in DoD. The study group also believes that the DIA/CIA balance is of value to the community: they have largely deconflicted their analysis and production, they have very different customer bases, and there is inherent value to maintaining the ability within the overall community to get a "second opinion." CIA correctly views one of its roles as providing an independent assessment of the efficacy of U.S. military operations. Although DIA has no formally constituted charter to challenge CIA assessments, in those areas that most threaten our national security, maintaining the ability to do competitive analysis is prudent, as long as it is by design and not a result of lack of management.

CIA and DIA, largely left to their own devices by the CMS but questioned by Congress repeatedly over a period of years for duplication of analysis and production, have made a great deal of progress in coordinating and deconflicting their analytical efforts and scheduled production. The fact that scheduled production represents a smaller and smaller percentage of total intelligence product in no way minimizes this achievement, but also shows that this process is a moving target. The coordination of finished products also does not address the issue of the community's other analytical products, which are not (theoretically) all-source -- SIGINT and IMINT reports.

Elements of the community have been moving independently in a positive direction in the analysis and reporting area -- this is both the good news and the bad news. The good news is that the community is using technology to work towards the types of products that are most useful to the customer: multi-source, multi-media products delivered electronically. The bad news is that this is being done in a largely uncoordinated way, resulting in the births of multiple, pseudo-all-source analysis centers using many of the same sources of data and producing products that look a lot like all-source products. What the community needs is a coordinated approach to distributed and collaborative analysis, similar to the concepts being developed at NSA

(the Analyst Driven SIGINT System being developed in conjunction with NIDL/Sarnoff Labs) and DIA (the Joint Intelligence Virtual Architecture, or JIVA). The community needs to create a "virtual analytical environment" that will maximize the efficiency of an increasingly scarce and valuable commodity -- the analyst. Although exploitation and first-level analysis should remain with the individual collection disciplines, many of the analysts currently doing SIGINT- and IMINT-centered analysis should be moved, physically or, preferably, electronically, to an all-source enclave (CIA or DIA) to provide the understanding of the source data and collection process required to produce high-quality all-source analysis and reporting, with appropriate feedback to the collectors/exploiters. By consolidating these efforts, we prevent the unnecessary replication of analytic effort by ensuring that this second- and third-tier analysis feeds directly into an all-source product, rather than resulting in an intermediate product that contains information from other sources but is not actually or officially all-source. This maximizes the productivity of the analysts and provides the customer with a faster and more comprehensive product.

The role of the CIA as the premier analysis and production agency should be reinforced. The DDCI who manages the CIA should also have primary responsibility for coordinating the community's analytical efforts, to include determining when and for what competitive analysis is justified. Most of the DCI's centers will remain in the CIA except for those associated almost exclusively with the current DO, which will become part of the Clandestine Service (see the *Intelligence Centers* staff study for more details). The CIA will also be the home of the National Intelligence Officers (although one or two may reside elsewhere, at DIA or State) and will be responsible for sponsoring the production of National Intelligence Estimates when they are warranted. The other role currently performed by the National Intelligence Council, that of evaluation, should be assumed by a new organization, the NIEC, which is independent of the CIA and is chartered to evaluate both analysis/production and collection against requirements. This evaluation activity needs to be linked directly to both the community requirements management, collection management and the program management activities (see the *Intelligence Requirements Process* staff study for more details), with the results of the evaluations going directly to the DCI, the DDCI managing the CIA, the DDCI for Community Management and the DMI.

Recommendations:

1) **Move towards a "virtual analytical environment" within the IC that electronically links collectors, exploiters, analysts, and, where appropriate, customers.**

2) **Move second- and third- tier exploitation and analysis, either physically or electronically, to the primary all-source analytical agencies, CIA and DIA.**

3) **Create a National Intelligence Evaluation Council (NIEC) for evaluating IC-wide collection and production, working closely with the Community Management Staff. The Head of the NIEC should be appointed by the DCI and report directly to him.**

VII. Planning, Programming, and Budgeting

The vast majority of the NFIP budget is embedded in the DoD budget. This was done partially for security reasons, in the case of the CIA, but there are practical and historical reasons for this as well. The DoD provides 86 percent of the personnel who conduct intelligence activities, both military and civilian. Of the statutory elements of the NFIP, only six do not belong to DoD: the CMS, the CIA, and the other Departmental elements belonging to the State Department, Justice Department (FBI), Energy Department and Treasury Department. The "fungibility" of defense dollars -- i.e., the fact that every dollar saved in intelligence can be used to fund other defense programs -- prompts concerns about the motivation of DoD (and Congress) to adequately fund intelligence in light of competing defense priorities. This raises the question as to whether it might not be better for intelligence and the nation to separate intelligence funding from defense funding, either completely or partially.

Attempting to separate the intelligence budget from the defense budget entirely would be extraordinarily difficult, and, philosophically, it is difficult to argue that intelligence does not belong in the defense account. In the view of the study group, under no circumstances is it practical or advisable to separate the joint and tactical intelligence programs from the rest of the force structure that they support, so, at most, it would be part or all of the NFIP that could be moved. However, we also believe that moving intelligence activities out of DoD would result in increased costs to the community that are now borne as services of common concern by DoD. Although the programs would be immune to the occasional across-the-board unallocated reductions applied to all DoD programs, the costs of not being part of DoD would probably far outweigh any savings in this regard. Another implication of this change would be that the total amount of the intelligence budget would, in all likelihood, have to be declassified. Although sound arguments can be made for declassifying the top line of the budget, and the SECDEF may make the decision to do this, the study group remains of the opinion that this would inevitably lead to the disclosure of more information about the IC than would be prudent.

If the goal of separating intelligence funding from the defense budget is to "protect" the NFIP, within the Executive Branch it is already, to all intents and purposes, protected. NFIP dollars, once identified, are effectively fenced. Executive Order 12333 tasks the DCI to:

"(n) develop, with the advice of the program managers and departments and agencies concerned, the consolidated National Foreign Intelligence Program budget, and present it to the President and Congress;
(o) Review and approve all requests for reprogramming National Foreign Intelligence Program funds, in accordance with guidelines established by the Office of Management and Budget;
(p) Monitor National Foreign Intelligence Program implementation, and, as necessary, conduct program and performance audits and evaluations." The National Security Act of 1947, as amended, states that the SECDEF shall:

> "(2) ensure appropriate implementation of the policies and resource decisions of the Director of Central Intelligence by elements of the Department of Defense within the National Foreign Intelligence Program."

DoD internal guidance (Carlucci memorandum of April 17 1981) stated the policy that NFIP "resources are 'fenced' and they are not to be increased, decreased, or transferred at any point in the fiscal cycle unless such action has been officially coordinated with the DCI." This policy is deemed to continue and has never been seriously challenged. Thus, the concept of the NFIP as a fenced program is well-established and accepted in the Executive Branch. The greatest risk to the NFIP comes from the Legislative Branch, which is currently free to "trade" intelligence dollars for defense dollars in the appropriations process.

One way to address this problem would be to create a separate line in the President's budget for intelligence. A separate line would lead to either an Intelligence and Defense Appropriations Bill or a completely separate appropriations bill (and appropriations subcommittee) for intelligence. However, separating intelligence from the rest of DoD (and, by inference, the other departments) into a separate appropriations bill, as was done with Military Construction some time ago, could well make the intelligence appropriations bill more vulnerable to political and fiscal winds, without the "cover" of the larger DoD appropriation. In all, the study group believes that it makes the most sense to leave NFIP funding in the various departments' budgets, but recommend a rules change within the House of Representatives that establishes some kind of a firewall between intelligence and defense funding in the appropriations process.

Assuming the intelligence budget is to remain in the defense budget, the question of how many mini-intelligence budgets there should be remains. There are currently three: the NFIP, the JMIP, and TIARA. Theoretically, the TIARA programs are service-unique and the JMIP programs support multiple services or the theater/JTF. It is an article of faith in DoD that the military services have the right to an organic intelligence capability as part of their force structure to serve their unique needs. The study group does not dispute this. This capability is logically composed of the programs grouped into the TIARA aggregation. The JMIP was established to provide

more centralized control over intelligence capabilities required for joint operations and that serve multiple customers. These programs are at the intersection between national and tactical intelligence and require a more intensive level of management to ensure that the boundaries are "seamless." There are, thus, logical reasons to retain both the JMIP and TIARA budget categories; however, their composition is a different issue.

The JMIP and TIARA budgets differ mostly in how they are constructed. Both are aggregates of MFP II programs, but while TIARA is merely the compilation of those intelligence and intelligence-related programs that the Services have elected to fund, the JMIP is constructed as a formal program and the role of the Deputy SECDEF as program executive protects the program from being "raided" by the Services. In practice, both the JMIP and TIARA are a hodgepodge of programs, the result of a series of unrelated and/or compromise decisions rather than a coherent plan. The composition of the NFIP, JMIP and TIARA was one of the nine key issue areas being examined for presentation to the Expanded Defense Resources Board (EDRB) for the fiscal year 1997 budget submission; it is to be hoped that the results of that review will rationalize the division of programs; regardless, the study group believes that further guidance is required for DoD on the appropriate composition of the JMIP and TIARA aggregation (see the *Congressional Oversight* staff study for jurisdictional implications of these divisions).

In addition to the policy and jurisdictional issues concerning the budget, there are serious problems with the mechanical process as well. The Community has long suffered from a vacuum in planning and guidance emanating from the DCI and his community-level staff. Although DCI guidance to the various functional managers is theoretically issued for each budget cycle, it is frequently either not done, not received in time, and/or not specific enough to affect the programming and budgeting of the various programs. In addition, the requirements system for the community, although much improved as a result of the evolution of the Needs Process, has never been successfully linked to the resource allocation process. Some of these issues are being addressed by the DCI and ExDir of the CMS. The NFIP budget has not previously been built in tandem with the DoD process; until fairly recently, there were not even agreed upon budget categories so that expenditures could be tracked across national and tactical programs. Assuming that most of the intelligence budget will remain a part of the defense budget, it is critical to apply similar processes to building the intelligence program and budget. The current ExDir's new programming and budgeting process is a positive step for several reasons. First, it rests the DoD portion of the intelligence budget on a foundation of program merit rather than relying on a good relationship between the DCI and the SECDEF. Second, it forces the IC itself to do a much more rigorous budget review than it has been able or tasked to do in the past, and to integrate its review with the non-NFIP defense intelligence programs, something that has never been done in a systematic way. It also puts the IC on a better footing with the Office of Management and Budget (OMB), which is beginning to play a more

active role in vetting IC budget submissions. Although this may or may not continue, it will always be a possibility depending on the inclination of each particular administration.

The disadvantage to this new process is perceived to be "greater DoD control" over the IC budget. However, the DCI and his staff control the development and review of issues and the composition of the program that is presented to the Expanded Defense Resources Board. Although all capabilities are included in the EDRB review process, formal budget action for the non-DoD programs is reserved for the DCI and review is done by the IC Executive Committee (EXCOM). Along with the rest of the NFIP, these activities are subject to OMB review. DoD has gained no new powers or authorities through this new process, only more visibility into some intelligence programs. As resources continue to be constrained, having DoD "buy-in" to the intelligence budget is not a bad thing. And, as has always been the case, in the final analysis the DCI has recourse to the President if he views the results of the process as unfair or inadequate.

A more subtle, but more important disadvantage to this process is that it is still the "tail trying to wag the dog." Currently, the program managers submit to the CMS a proposed budget based on top-line guidance from the DCI that has been coordinated with the SECDEF. The CMS does a largely surface review of the submissions (often by personnel on temporary rotation from the agencies they are reviewing) and may make some minor changes to accommodate DCI priorities or some of the more vocal issue coordinators. When the budget is finalized, it is sent to Congress as part of the President's Budget. When the Congress authorizes and appropriates the money, it is appropriated directly to the program managers. The CMS has no control over -- indeed, no visibility into -- budget execution. If the DCI is to manage the Community as a corporate entity and ensure that resource trades are made to address priorities, he and his staff need more authority in the intelligence budgeting process.

Although IC funding should still be appropriated to the various Departments, the CMS must have formal authority for formulating the NFIP budget, including the ability to monitor execution, withhold funds and reprogram funds within the NFIP. Thus, the elements of the NFIP should provide budget inputs to the CMS, but the CMS should build the budget in the functional categories mentioned above and submit the Congressional Budget Justification Books (CBJBs) to Congress. The authority to reprogram should be limited to not more than five percent of the losing agency's budget over a one-year period, subject to normal OMB review. The ability to withhold funds as a result of execution review should be accomplished by a formal arrangement between the DCI and SECDEF, allowing the CMS to identify to the OSD comptroller funds to be withheld. These recommendations require the CMS to be significantly enlarged, and although rotational personnel should continue to provide manpower and expertise to the staff, it must have a robust cadre of core staff to perform these and other functions recommended in this staff study.

The single most important change that needs to be made concerns the organizing principle around which the budget is constructed. Broadly speaking, the budget could be organized around programs, missions, disciplines or functions. Notwithstanding the existing budget structural categories, the current budget is constructed around programs, even though each program varies widely in mission and composition. Almost any other solution would be an improvement; however the study group believes that the most constructive way to build the budget is along functional rather than programmatic or discipline lines, in the broad categories of collection, processing and exploitation, analysis and production, and infrastructure (to include R&D, dissemination, etc). Building the budget this way would force the types of trade-offs between like items that the IC has been largely unable to achieve to date, and would eliminate the current hegemony of the program managers in the budget process. It would also present to Congress a more balanced picture of the budget and the resource trades made to accommodate changing priorities. Building the budget around disciplines hinders the cross-discipline trades that need to occur, and building it around missions is difficult, because so many capabilities serve multiple purposes. While clearly any budget must start with missions and the required capabilities to perform them, the budget would more constructively be built around those capabilities rather than the missions themselves.

Complicating the achievement of this goal is the community method of budgeting and accounting itself. Although there are standard budget accounting categories for the community, each program defines these categories somewhat differently and has its own unique budgeting and accounting system and infrastructure. In addition, resource data are retrievable *only* under the established budget categories, so there is no efficient way to do cross-mission or cross-functional analyses -- for example, to determine how much the community as a whole is spending on computer support. The Committee has several times engaged the CMS in discussions about how to do matrixed cost accounting so that resources could be flexibly associated with more than one category, but designing and implementing a system for the community that would meet those needs while allowing the DoD agencies to maintain necessary compatibility with DoD is not a trivial undertaking. If the CMS is given both the responsibility and the authority for building the NFIP program and conducting execution reviews, as it should be, a new programming, budgeting and cost accounting methodology must accompany these changes, which will standardize programming and budgeting procedures across the IC.

Recommendations:

1) **Retain but rationalize the NFIP, JMIP, TIARA budgets. Provide guidance to DoD concerning the appropriate composition of JMIP and TIARA.**

2) **Provide the CMS a program analysis and evaluation (PA&E) and a limited comptroller capability which would allow them to take responsibility for formulating and executing the NFIP budget.**

3) **Provide the DCI limited authority to reprogram funds within the NFIP, the amount not to exceed five percent of the losing agency's budget for a one-year period (Section 14(d) of the National Security Act).**

4) **Provide the CMS the ability to withhold funds through an arrangement with the OSD comptroller.**

5) **Mandate that the budget be built along functional rather than programmatic lines. Mandate and fund a new community programming, budgeting and accounting system that can track resources in multiple categories across the IC.**

VIII. Personnel Management

The IC continues to face a major personnel crisis that it has, thus far, not addressed in a coherent way. The mandated downsizing, conducted as it has been on a voluntary basis, has left holes in the workforce that cannot be filled because there is no head room to hire new people. The demographic profiles of NSA and DIA are a disaster waiting to happen in 5-10 years unless some way is found to maintain a steady infusion of new blood into the community. At the same time that the number of personnel is declining, the cost of the remaining personnel is continually increasing, meaning that there has been little if any real savings associated with this painful process. As mentioned earlier, the focus of our global interest is changing and requires a different skill mix than the preponderance of political and military analysts that were the bread-and-butter of the Cold War.

A related issue that cannot be ignored indefinitely is morale. Without the creation of some head room, prospects for promotion are grim. Without a reasonable demographic spread, meaningful career development is virtually impossible. Again, resolving these problems is dependent at least in part upon the ability to reduce the current workforce faster and more selectively than the hitherto voluntary, incentivized approaches. Further eroding morale is the lack of clear standards in some agencies and the perception of unfair advancement of certain segments of the population. A viable performance appraisal system across the community is an important step to improving this situation.

Much of the discussion about the problems in the IC, and particularly the CIA, has revolved around the culture of the community and how it needs to change. However, it is difficult to change a culture by simply moving the same people around in an agency. New blood and fresh perspectives are required, and they can be

attained in two basic ways: hiring new people, or "borrowing" people from other agencies and sending your people to those agencies so they come back with some new ideas. The IC overall needs to develop a "corporate culture," and it needs to do this primarily through personnel reform that promotes the concept of a community of professionals rather than a loosely connected group of agencies between which personnel movement is very difficult, if not impossible. This was the whole idea behind the personnel provisions of Goldwater-Nichols, which was designed (largely successfully) to break down the walls between the insular service personnel systems and promote a culture of "jointness."

There have been numerous studies done on personnel management in the IC. As is pointed out in the report of the most recent Intelligence Community Task Force on Personnel Reform, led by Christopher Jehn, the same recommendations have been made again and again, but never implemented. In the past, the community has been unable to overcome the resistance of agencies or individuals to address personnel policy issues at the community level. However, we understand that the DCI and the Administration are drafting a legislative proposal for inclusion in the fiscal year 1997 authorization bill that incorporates the recommendations of the Jehn report. The study group is prepared to endorse all of these recommendations, particularly the requirement for an effective performance evaluation system and a coherently managed personnel system that would promote rotations and lateral movement within the community.

The Jehn report states that in the course of the task force's review of current personnel systems in the IC, "four principal problems emerged:

1) a largely dysfunctional system of performance appraisal and management;

2) a lack of systematic career planning and professional development across the IC;

3) the variety and complexity of the various systems; and

4) inadequate promotion of a sense of community among the agencies, including a lack of tools and incentives for managers to promote diversity and make full use of the intellectual and cultural diversity in the IC's workforce."

The task force's recommendations to counteract these problems were:

1) create an effective performance management system, encouraging the adoption of common performance criteria and standards across agencies;

2) employ broadbanding for compensation and position management to give more flexibility to local managers and immediate supervisors;

3) adopt a system of systematic initial appointment and separation management;

4) standardize recruiting practices, much of career training and elements of the performance management system across agencies, to include a career development program that includes joint training, rotational assignments, and dual tracks for substantive experts and managers.

It is important to emphasize that a performance management system would not be identical for each agency or skill area. However, community-wide standards for performance appraisals, compatible pay banding systems, centrally-managed personnel security and a career development program are essential elements for reducing duplication and facilitating lateral movement within the community, thus promoting jointness and improving morale. At a minimum, the SES system should be standardized at the community level, and a rotational assignment should be a prerequisite for achieving SES rank except in rare circumstances. Dual tracks should be available for those personnel who do not aspire to high levels of management but would rather remain in specialized areas such as clandestine operations or cryptomathematics. In addition, we believe the DCI should be able to detail personnel within the community as required to meet short-term surge requirements (see *Intelligence Community Surge Capability* staff study). However, this authority should be limited to no more than 180 days without the concurrence of the parent agency.

The issue of how to reduce further the numbers of personnel is a complicated one and no single solution will effect the required change. Many of the recommendations in the Jehn report would, over time, improve the community's ability to identify and terminate poor performers, particularly if the DCI's termination authority were expanded to the entire community. The problem is how to address the critical time period of the next 2-5 years before these recommendations, if implemented, could begin to have an effect.

The agencies of the IC already have certain expanded authorities beyond those accorded to other government agencies. They have termination authorities (although only the CIA has a truly unambiguous termination authority), but they have no special RIF authorities or exemptions from the rules governing RIFs of civil service personnel. The termination authorities are not currently used for fear of lawsuits, a not unreasonable fear in the absence of a performance appraisal system that could produce a documentary record and justification for action. Limited legislative authorities, such as the two percent waiver and directed retirements of annuity-eligible personnel, could provide some relief but could be extremely difficult to get through Congress because of jurisdiction, fiscal and legal challenges. These programs need to be approached as pilot projects with the full cooperation of OMB in order to have some chance of being instituted, and even then cannot be guaranteed. However, it is the belief of the study group that the importance of this issue makes these efforts worth making and we recommend legislation for the Fiscal Year 1997 Intelligence

Authorization Act establishing pilot programs for the two percent waiver and directed retirement of annuity-eligible personnel. Proposals for one-time dispensations to either reduce personnel or temporarily exceed mandated downsizing goals in order to allow hiring of essential new personnel were rejected because, although they may be effective in the short term, they do not provide the DCI with tools to prevent a recurrence of the current situation and to enable to IC to continually restructure its workforce in response to changing priorities and targets.

Recommendations:

1) Implement recommendations of the Intelligence Community Task Force on Personnel Reform.

2) Standardize SES system across the community and make a rotational assignment a prerequisite for SES rank.

3) Authorize pilot programs to further reduce numbers of intelligence personnel, to include the waiver of the two percent retirement penalty and directed retirement of retirement-eligible personnel.

4) Provide the DCI enhanced control over NFIP personnel, to include the ability to detail as required for up to 180 days.

IX. Research, Development and Acquisition

Numerous interviews, panels and hearings confirmed the need for better management of increasingly scarce R&D dollars. Reports by an independent review panel on NSA's Advanced Research and Development Program, the results of the Exploitation Technology Working Group's review of R&D efforts in the imagery processing and exploitation field, and a wealth of anecdotal information support the contention that advanced R&D efforts are not adequately focused on the highest priority technical problems facing the IC. The individual discipline staff studies identify the critical areas requiring attention. Currently, although there is an individual on the CMS charged with looking at Advanced Technologies, R&D efforts remain fragmented under the control of individual program managers. The community coordinator has no budgetary authority and, thus, a limited effect on the various programs of the community.

The various R&D efforts in the community require closer coordination with the requirements management element to ensure that R&D dollars are focused on the problems that are the most critical, not the most topical or the easiest. It is the study group's belief that the community also needs an R&D fund, similar to the Military Exploitation of Reconnaissance and Intelligence Technology (MERIT) program run by the NRO, to fund promising R&D projects. Under this concept, a fund would be

established and elements of the IC could submit proposals on an annual basis for low-cost, potentially high pay-off technology demonstrations or experiments. These would be evaluated by a formally constituted review board and the available funds allocated to the projects based on merit. The MERIT program has been an extremely effective, albeit limited, response to the conundrum within DoD that it is harder to get $2 million now for a good idea than to get a $20 million project into the planning cycle for two years down the road.

Another issue that must be addressed by the IC is the cumbersome acquisition process and the need to find a way to keep pace with commercial technology developments, particularly in the automation area. Each agency has automation plans and recapitalization plans of varying degrees of effectiveness. The result is that the community has a bewildering mixture of automation support hardware and software, almost none of it compatible and little of it state of the art. An important function of the ISO, mentioned earlier, would be to establish standards and information architectures for the entire community, building on the role played by the Intelligence Systems Board today. The community also needs a centralized fund for the life-cycle replacement and upgrade of community automation equipment, and a contracting vehicle that does not require the full-blown DoD procurement process to be followed.

Consistent with the move towards corporateness and consolidation where practical and efficient, the study group believes that many R&D and acquisition activities should be consolidated for greater efficiency and coherence. Portions of the NRO would form the core of a new agency, but its scope would be broadened to include development of all reconnaissance systems, including airborne systems, and the sensor development and acquisition activities currently undertaken by the Directorate of Science and Technology (DS&T) within the CIA. This agency would be called the Technology Development Office (TDO) and would be funded via the NFIP and the JMIP (for programs currently within the Defense Airborne Reconnaissance Office (DARO)). The inclusion of the DARO in this concept would facilitate the development of a truly unified air/space reconnaissance architecture, an elusive goal thus far. The TDO would have Section 8 acquisition authorities for NFIP monies to ensure that the NRO's and CIA's traditional ability to conduct streamlined acquisition is not lost, and would serve as the acquisition executive with milestone approval authority for the DARO programs. As with most of our IC21 proposals, this would not necessarily require the physical relocation of these elements, but would rely upon a unified management approach to the overall reconnaissance architecture and sensor R&D arena.

Other areas of R&D, such as those conducted at NSA in the signal processing area and specialized R&D in support of clandestine HUMINT operations, would remain associated with the agencies they specifically support, but come under greater management review in the process of building the budget functionally. The imagery and MASINT processing R&D currently done at the NRO and DS&T would migrate to

the TCA.

Recommendations:

1) Create a Technology Development Office that combines R&D and procurement functions for reconnaissance and sensor technologies, to include elements of the NRO, DARO, CIA, and NSA. Maintain Section 8 authorities for NFIP funds; serve as acquisition executive for DARO programs.

2) Establish a MERIT-like contingency fund for the IC to exploit technological targets of opportunity.

3) Establish a fund and a funding mechanism for rapid and continuous update of information systems and automation technologies.

4) Empower the Infrastructure Support Office (ISO) to establish standards and develop architectures for the IC. Make the ISO responsible for the life-cycle management of community ADP systems.

INTELLIGENCE REQUIREMENTS PROCESS

Executive Summary

Findings

The Intelligence Community, with all its components and disciplines, needs an overarching concept for coordinating Community requirements, especially when faced with declining resources and increasingly diverse requirements.

The Needs Process

With its focus on Presidential Decision Directive - 35 (PDD-35), the National Needs Process is an important step towards dealing effectively with near-term, high-priority customer requirements, but it may be inadequate for meeting long-term, worldwide intelligence needs, primarily because PDD-35 has begun to drive collection and analysis at the expense of lower tier issues.

Defining Future Intelligence Needs

The Intelligence Community has, correctly, changed its focus and targeting since the end of the Cold War, but it cannot link long-term resource planning to future needs until it defines what its future intelligence needs will likely be.

The Intelligence Community cannot base its long-range planning primarily on high-level policy maker-defined requirements because policy makers, by their very nature, tend to concentrate on immediate problems and do not think long-term.

Focus on Top Tier Issues--Creating Intelligence Gaps?

We are concerned that, with declining resources, collectors and analysts will continue to focus most resources on top PDD-35 priorities and assume that "someone else," (i.e., State Department, FBIS, etc.), has the resources to keep a minimal level of coverage on lower tier issues.

Losing our Intelligence Base

The Intelligence Community's ability to maintain an intelligence "base" on many lower tier issues is threatened not only because of PDD-35's unintended effect on collection and production, but also because the Intelligence Community currently has no mechanism to ensure that a basic level of coverage for all issues is maintained.

Support to Military Operations (SMO)

The demand for intelligence support to military operations (SMO) threatens to consume an increasing amount of Community resources at the expense of national intelligence needs.

Level of Engagement with Policy Makers

In order to best meet its customers' requirements, the Intelligence Community must work actively with policy makers to disaggregate their intelligence needs into smaller, actionable parts. Policy makers, in turn, must strive to articulate policy strategies and objectives more clearly to the Intelligence Community.

Analysts and managers at lower levels must maintain informal contacts with their customers, because often, mid-level policy makers can provide in-depth knowledge and further detail for a particular policy need.

Budgetary Authority

Program managers have a disproportionate level of power over resource and programming issues vis-a-vis Issue Coordinators, many of whom have little knowledge about the budget process and collection resource issues. Thus, Intelligence Community budgeting tends to meet systems requirements rather than information needs.

"Cross-INT" Coordination

The Intelligence Community does not manage all-source collection well, leading to inefficiencies and sometimes unnecessary duplication in meeting customer needs. The establishment of an enhanced Community Management Staff (CMS) (see *Intelligence Community Management* staff study) with requirements, resource, and collection management authority would enable the Intelligence Community to more efficiently meet Community-wide requirements.

Requirements Committees

There is no formal, ongoing dialogue among the various requirements committees, and as a result, no overarching, corporate view of the Community collection process against requirements targets.

Recommendations

Community-Wide Approach

The Director of Central Intelligence (DCI), in coordination with the CMS requirements office, should devise a strategic plan, that could be updated yearly, if necessary, outlining national security issues and gaps which the Intelligence Community will likely face 10 to 15 years into the future.

Basic Worldwide Coverage

The Intelligence Community should fulfill PDD-35 requirements, but also maintain a basic level of worldwide coverage. In order to ascertain the Community's current level of *overall* coverage, the DCI should direct the National Intelligence Evaluations Council (NIEC) to expand the "Comprehensive Capabilities Review" to evaluate collection and analytical capabilities and gaps against *all* tier issues. The review should be updated continuously, taking the DCI's strategic plan into account.

Based on the capabilities review process, the Intelligence Community, under the auspices of an enhanced CMS should assign specific collection and analytical components responsibility for some basic level of coverage of lower-tier countries and issues.

Cross-INT Coordination

The establishment of a new Technical Collection Agency (see *Intelligence Community Management* staff study) would facilitate coordination among the various collection disciplines and improve efficiency in meeting intelligence requirements.

Requirements Vision for the 21st Century

The Intelligence Community should implement a "virtual analytic environment" linking collectors, exploiters, analysts, and customers electronically, as appropriate, to improve the Community's responsiveness to customer needs.

As a model for achieving electronic connectivity, the Intelligence Community should look to the military's test-bed programs for creating a 21st century intelligence operating environment. This operating environment, known as JIVA (Joint Intelligence Virtual Architecture), focuses on creating a virtual work environment that transcends organizational and stovepipe boundaries. A virtual architecture will allow analysts and collectors to more efficiently work requirements and maintain continuous contact with policy makers. This will also allow the policy and intelligence communities to constantly refine requirements and refocus resources on those issues of paramount importance.

Managers should function less as intermediaries who control the information flow to and from policy makers and more as facilitators who monitor the dialogue between policy makers and substantive experts. Managers also should ensure that intelligence does not become politicized as a result of the close analyst-policy maker working relationship.

INTELLIGENCE REQUIREMENTS PROCESS

Scope of Paper

This paper takes a macro look at the Intelligence Community requirements process, specifically, the current structure and future applicability of the National Intelligence Needs Process. The requirements study examines the overall process of formulating requirements, rather than the specifics of how the specific collection disciplines, or "INTs," should be used to meet these requirements in the future. This study provides guidelines to the Intelligence Community on how the requirements process should be structured to ensure that the Community can meet national security needs of the 21st century.

Introduction

The principal mission of the Intelligence Community is to supply policy makers with timely information and analysis that allows for informed, knowledgeable decisionmaking. In order to fulfill this mission, the Intelligence Community must understand the prioritized intelligence requirements of policy makers. These requirements should not only play a central role in defining the mission, functions, and structure of the Intelligence Community, they also should drive the Community's collection, analysis, and budget. In an ideal world, the Community would be able to fulfill all actual and potential policy maker requirements in a timely, comprehensive manner. Unfortunately, the requirements process is complicated by the fact that it is often difficult for senior policy makers to focus on long-term intelligence requirements because they usually are occupied with more immediate, pressing issues and because, in many cases, they do not know what information they want until they actually need it. In addition to the difficulty of eliciting policy maker needs, there are political, bureaucratic, and resource realities that hinder the Community's ability to anticipate and satisfy all intelligence needs.

The United States has lacked a strategic vision defining its role in the world since the end of the Cold War. The requirements process, in fact, has been made even more difficult by the absence of any current political consensus on national security issues and their importance. As policymakers have struggled to define core national interests, they have turned to the Intelligence Community for increased coverage of diverse issues. Because of the changing--but not clearly defined--nature of threats and intelligence needs since the end of the Cold War, the Intelligence Community itself has been forced to reexamine its roles and missions. There is considerable disagreement among experts about whether the Intelligence Community

should focus primarily on supporting national security policy makers or whether it should support other customers, such as law enforcement agencies, economic/trade officials, or environmental agencies. Still others argue that intelligence support to military operations (SMO) should be the primary function of intelligence. These debates over national security priorities and the Community's mission, requirements, and customer base are not easily resolved. Nonetheless, the Intelligence Community's function in aiding the national security decisionmaking process must be defined so that it can properly target its resources against the most important foreign policy challenges.

Ideally, requirements should reflect policy makers' prioritized intelligence needs and help the Community devise long-term planning and investment strategies. However, without a strategic national security policy vision to guide it, the Intelligence Community often is forced to prioritize requirements itself. In addition, because policy makers often do not know what intelligence they need or want until they actually need it, the Intelligence Community must try to anticipate policy maker needs. This can only be achieved if the Community, through an ongoing requirements dialogue with senior policy makers, sets the minimum collection and analysis parameters not only for the most important, immediate strategic needs, but also for long-term needs. Experienced mid-level analysts also should be allowed to formulate requirements based on their expertise and through constant dialogue with policy makers at various levels, as well as with intelligence collectors and other analysts. Unfortunately, the Community's bureaucratic structure often impedes this type of free-flowing dialogue and interaction at the working level.

In addition to political and bureaucratic issues, resource concerns also have an effect on the Community's ability to meet policy maker requirements. In the post-Cold War era, requirements have become increasingly diverse; at the same time, the Community has been forced to downsize considerably. Despite fewer resources, the Intelligence Community is expected to have at least basic worldwide coverage of most countries and issues while maintaining in-depth knowledge of high-priority issues. In order to achieve this level of coverage, the Intelligence Community may have to pursue a dual requirements strategy to deal with increasing requirements -- a day-to-day one with good breadth, but little depth, to cover usual areas of interest, and a second one with narrow focus and great depth for crises or issues of ongoing, intense interest.

Maintaining an effective requirements process has been a continuous struggle for the Intelligence Community. During the Cold War, when a majority of Community resources were targeted against the Soviet Union, having an effective requirements process was less important than it is now. Since the end of the Cold War, the growing tangle of new requirements, some of which are of the "highest priority" for

only a short time, has left the Intelligence Community without clear guidance on which to base its resource allocation and planning. Lacking a cohesive foreign policy strategy to guide it and faced with declining resources and increasingly diverse customer demands, the Intelligence Community needs a flexible, dynamic requirements process to help it fulfill its principal mission -- to provide policy makers with timely, useful, objective intelligence.

Background: The Requirements System Today -- The National Needs Process, PDD-35 and Strategic Intelligence Reviews

The current system for intelligence requirements, known as the "Needs Process," is derived from Presidential Decision Directive-35 (PDD-35), signed by the President in March 1995, and the "Strategic Intelligence Reviews" (SIRs), first published by the National Intelligence Council (NIC) in May 1994. The SIRs identify core near-term (12-18 months) intelligence issues, priorities, and gaps for various geographic regions and transnational issues and assess the value of current collector contributions against those issues. The SIRs also identify "enduring" intelligence needs (i.e., of concern for the next three to seven years) to help program managers do long-term budgeting. PDD-35, which outlines a tiered structure of the President's prioritized intelligence needs, provides collection and analysis guidance to the Intelligence Community. After PDD-35 was signed, an interagency task force made recommendations on how to align "enduring" intelligence challenges with the PDD-35 tier structure.

The responsibility for writing the SIRs belongs to 18 Issue Coordinators who meet frequently with high-level policy makers.[1] The function of Issue Coordinators is to understand key customer needs, develop a prioritized statement of those needs, evaluate the current collection and analytical activities related to those needs, assess the intelligence value of future programs, and facilitate community responses to critical shortfalls. In the process of writing the most recent set of SIRs (November 1995), Issue Coordinators met with over 100 high-level intelligence consumers[2] in order to get an understanding of their most important needs.

---

[1] The Issues Coordinators are the National Intelligence Officers (NIOs) from the NIC, the Center Chiefs (ACIS, CNC, NACIC, and CTC), and "key officers" from the Defense Intelligence Agency (DIA) and the Joint Chiefs of Staff (JCS).

[2] Throughout the paper, the terms customer, consumer, and policy maker are used interchangeably to refer to those U.S. Government officials who use intelligence products in the course of their work.

Findings

The Needs Process

The Intelligence Community, with all its components and disciplines, needs an overarching concept for coordinating Community requirements, especially when faced with declining resources and increasingly diverse requirements. Leadership from the highest levels of the Intelligence Community is necessary to ensure that policy makers' most important needs are being met and that the Community is poised to cope with the intelligence challenges of the 21st century. With its focus on PDD-35, the National Needs Process is an important step towards dealing effectively with near-term, high-priority customer requirements, but it may be inadequate for meeting long-term, worldwide intelligence needs. In fact, if the Intelligence Community focuses primarily on policy maker-defined requirements, it cannot adequately prepare for the needs of the future because policy makers, by their very nature, tend to concentrate on immediate problems and do not think long-term.

Defining Future Intelligence Needs

The Intelligence Community has, correctly, changed its focus and targeting since the end of the Cold War. It cannot however, hope to link long-term resource planning to future needs until it has a corporate understanding of what future intelligence needs will likely be and how its resources currently are used to meet intelligence requirements. Although there is disagreement about what will constitute a threat to U.S. national security in the future, the Community must, at a minimum, be capable of dealing with issues such as foreign denial and deception, proliferation of weapons of mass destruction, terrorism, ethnic and regional conflict, and economic competitiveness. Throughout the Cold War, the Intelligence Community could design systems aimed at country-specific targets, (i.e., "denied areas"), but the national security needs of the future do not allow us to look at resources on a strictly nation-state basis. Indeed, the Community must still plan for meeting requirements on "enduring" hard targets, such as North Korea. However, the Community also must design, invest, and plan its future systems and capabilities around "types" of threats, such as proliferation, rather than around specific threats necessarily tied to a particular country or region.

Focus on Top Tier Issues -- Creating Intelligence Gaps?

Under any system that prioritizes requirements, collectors and analysts will naturally put most resources towards the highest priority issues. While PDD-35 has focused the IC on important near-term, high priority requirements, it has begun to drive intelligence collection and production at the expense of lower tier issues. In

response to PDD-35, many intelligence agencies and components are rushing out to fulfill PDD-35 requirements while ignoring other, less pressing requirements, even when they are better equipped to address the lower tier requirements. If PDD-35 continues to drive the intelligence process, the Community may face another Rwanda or Somalia situation -- that is, a country that had little, if any, intelligence coverage suddenly becoming a top tier priority.

Although PDD-35 explicitly states that it is not meant to be an exhaustive requirements list, we are concerned that, with declining resources, collectors and analysts will continue to focus most resources on top tier issues and assume that "someone else," (i.e., State Department, Foreign Broadcast Intelligence Service (FBIS), etc.), has the resources to keep a minimal level of coverage on lower tier issues. The Intelligence Community cannot necessarily rely on other government agencies to fill its own collection gaps because the State Department, like the Intelligence Community, is being downsized and seeing reductions in its diplomatic reporting capabilities. In addition, in many of these lower-tier countries, particularly those in the Third World, open sources are often inadequate and inaccurate sources of information. Furthermore, FBIS has not been spared from downsizing and is also concentrating its efforts on top tier issues.

Losing our Intelligence Base

The Intelligence Community's ability to maintain an intelligence "base" on many lower tier issues is threatened not only because of PDD-35's unintended effect on collection and production, but also because the Intelligence Community currently has no mechanism to ensure a basic level of coverage for all tiers. In addition, the demand for SMO threatens to consume an increasing amount of intelligence resources at the expense of national intelligence needs. With the erosion of our intelligence "base," (i.e., the ability to monitor political, military, economic, and social developments around the world), comes serious consequences for the Intelligence Community's ability to "surge" and do long-term analysis. Under the current Needs Process, there is no corporate view of collection and production management that is necessary to ensure that collectors maintain databases of lower tier information and that enough analysts are available to monitor lower-tier issues and potentially important long-term trends. Maintaining an intelligence base is particularly critical when, as we have experienced several times in the recent past, lower tier countries rapidly and unexpectedly become top priority issues for policy makers.

Support to Military Operations

In addition to fulfilling numerous top priority requirements, collectors and analysts are expected to develop and/or update data for lower-tier countries where

U.S. forces may have to operate in the future. SMO certainly is an extremely important mission for the Intelligence Community. However, the effort required to obtain detailed information sufficient to support short-notice military operations in scores of countries would strain the Community's ability to stay abreast of more pressing issues. In addition, the proposal that the military define the "essential elements of information" it needs for potential operations in these countries raises the specter of an endless list of requirements being levied on the Intelligence Community. In order for the Community to be able to cope with SMO requirements, the level of detail needed for SMO in lower-tier countries must be strictly defined. Furthermore, SMO requirements should not stand alone, apart from the other intelligence requirements. Currently, the Needs Process demands, in some cases, that the Community spend more time gathering intelligence for potential SMO than for monitoring other developments that might help policy makers avert the need to ever have to deploy forces. If a country is important enough to have SMO requirements assigned to it, then national intelligence consumers also should have enough information to assess the country's general economic, political, and social situation.

Level of Engagement with Policy Makers

Under the current system, most Issue Coordinators have ongoing communication with high-level policy makers about strategic policy goals, which are then formulated into overall Community-wide requirements. Issue Coordinators attend National Security Council (NSC) meetings frequently and typically meet with intelligence customers at the Undersecretary or Deputy Secretary level at the State Department and the command level in the Department of Defense (DoD). While high-level contact is vital to the requirements process, analysts and managers at lower levels must maintain informal contacts with their customers because, often, mid-level policy makers can provide in-depth knowledge and further detail for a particular policy need. This type of informal dialogue also must exist between collectors and analysts and among analysts in different Community components.

Policy Detail

Just as important as the need for constant Intelligence Community dialogue with customers is the need for the Community to understand the details of policy makers' goals. The Community must work actively with policy makers to disaggregate their intelligence needs into smaller, actionable parts and should understand how policy makers plan to use the intelligence they receive so it can devise the most appropriate collection strategy to satisfy that need. With an issue such as proliferation, for example, different collection assets might be used depending on whether the policy goal is to intercept weapons shipments, influence key foreign

leaders to not proliferate, apply sanctions against a proliferator, or simply to monitor developments in a country's weapons industry.

Budgetary Authority

We are concerned that program managers--whose interests focus more on their share of the budget than on fulfilling policy maker requirements--have a disproportionate level of power over resource and programming issues. Many Issue Coordinators, particularly the NIOs, are not knowledgeable about the budget process and collection resource issues and lack sufficient staffs capable of handling these issues. As a result, they have to rely on program managers more extensively to reprogram resources in surge situations and to set future systems requirements. This power imbalance has resulted in the Community budgeting to meet systems requirements rather than information needs, which may adversely affect the Community's ability to fulfill policy maker requirements.

"Cross-INT" Coordination

Another concern about the Needs Process is the issue of cross-INT coordination. (This issue is dealt with in detail in the *Collection Synergy* staff study, but merits some attention here as well.) The Intelligence Community does not manage all-source collection well, leading to inefficiencies and sometimes unnecessary duplication in meeting customer needs. Management by "stovepipes", rather than across disciplines (i.e., corporately), makes it difficult, if not impossible, to evaluate collection tradeoffs, not only within collection disciplines, but among them as well. Cross-INT coordination would be especially helpful for dealing with "hard targets," which often require coordinated, multi-disciplinary attacks.

Requirements Committees

A related issue of concern is the level of communication and coordination among the various committees that handle requirements for each of the collection disciplines. The requirements committees meet with each other informally three to four times a year to discuss how various collectors are approaching a particular intelligence need, but there is no formal, ongoing dialogue and, as a result, no overarching view of the Community collection process against requirements targets. Further complicating coordination efforts is the fact that the requirements committees have different missions and authorities; some committees have the authority to task collectors while others only have the authority to request reporting on various topics.

Recommendations

Community-Wide Approach

The Intelligence Community must define the nature of its future strategic requirements, beyond looking just at intelligence gaps, in order to determine what platforms will be needed to meet those requirements. The DCI, in coordination with the CMS requirements office, should devise a strategic plan, that could be updated yearly, if necessary, outlining national security issues and gaps that the Intelligence Community will likely face 10 to 15 years into the future. It should include, but not be limited to, hard targets and transnational issues. In addition to looking at traditional adversarial threats (i.e., states and organizations with the ability and will to harm U.S. interests), the Community must focus on how to collect against systemic threats (i.e., those which derive from anomalies or instabilities in economic, political or social systems) and against new vulnerabilities, such as information warfare. Based on this strategic plan, the CMS requirements office, with input from senior intelligence customers and all-source analysts, should formulate Community-wide requirements and devise a collection strategy to meet those needs. By preparing a strategic plan for the future, the Intelligence Community can assist policy makers in prioritizing their own needs.

Basic Worldwide Coverage

The Intelligence Community must maintain its intelligence base and its ability to surge. We are well aware of the fact that many Intelligence Community components already are stretched to the limit in handling top-tier issues and that the situation will likely get worse in some agencies because of restricted hiring practices. At the same time, however, many in the policy community still expect the Intelligence Community to have at least basic worldwide coverage and the ability to surge at a moment's notice during crises. In order to ascertain the Community's current level of *overall* coverage, the DCI should direct the National Intelligence Evaluations Council (NIEC)[3] to expand the "Comprehensive Capabilities Review" to evaluate collection and analytical capabilities and gaps against *all* tier issues. The review should be updated continuously, taking the DCI's strategic plan into account. Assessing intelligence capabilities on an ongoing basis will help bring policy maker expectations into line with Community capabilities and will serve as a mechanism for facilitating cross-INT tradeoffs to ensure that the most important areas are covered by collectors and analysts. A dynamic capabilities review process also would be extremely helpful for the Committee in dealing with budgetary issues and for other congressional committees with jurisdiction over national security and international relations issues.

---

[3] See the *Intelligence Community Management* staff study.

Based on the capabilities review process, the Intelligence Community, under the auspices of an enhanced CMS,[4] should assign specific collection and analytical components responsibility for some basic level of coverage of lower-tier countries and issues. Because open source information may be the most accessible, least expensive tool for obtaining worldwide coverage, the Community should work with the State Department to coordinate diplomatic and open source collection. FBIS's ability to collect and analyze adequate information for lower-tier countries also should be evaluated so that the Intelligence Community and Congress can determine what additional resources FBIS will need in the future to meet this important mission. A healthy FBIS is needed to rebuild some of the Community's lost capabilities resulting from the cutbacks in the CIA and State Department's overseas presence.

Cross-INT Coordination

In order to encourage efficiency in meeting intelligence requirements, the "catwalks" among the collection disciplines must be strengthened. The establishment of a new Technical Collection Agency (TCA)[5] would facilitate coordination among the various collection disciplines and improve the Community's responsiveness to policy maker needs. An enhanced CMS, through coordination among its proposed requirements, collection management, and resource management offices, would serve as the forum for ensuring that synergistic, cross-INT coordination is utilized to best meet requirements.

Requirements Vision for the 21st Century

The above recommendations are important for effecting immediate change in the current requirements system. However, the Community must go even further to prepare for challenges it will face 10 to 15 years into the future. The Community probably will still need a high-level body to formulate and monitor macro community-wide requirements that provide important guidance to program and agency managers. However, mid-level analysts, working in close and continuous contact with policy makers, collectors, and other analysts should be allowed to work detailed requirements. In order to empower analysts to help develop these detailed requirements, analysts must be connected electronically at all levels with both policy makers and intelligence collectors. (Analysts should serve as the middleman between

---

[4] See the *Intelligence Community Management* staff study.

[5] See the *Intelligence Community Management* staff study.

policy makers and collectors; collectors and policy makers working non-military issues should not be connected electronically.)

As a model for achieving electronic connectivity, the Intelligence Community should look to the military's test-bed programs for creating a 21st century intelligence operating environment. This operating environment, known as JIVA (Joint Intelligence Virtual Architecture), focuses on creating a virtual work environment that transcends organizational and stovepipe boundaries. A virtual architecture, that eliminates the need for physically co-locating analysts, will allow analysts and collectors to more efficiently work requirements and maintain continuous contact with policymakers. Breaking down these barriers will help synergy in all areas -- collection, analysis, production, and requirements formulation and vetting. By providing more flexibility and less bureaucratic rigidity, electronic connectivity will allow the policy and intelligence communities to continually reevaluate requirements and refocus resources on those issues of paramount importance. At the same time, by co-locating analysts with policy makers, either virtually or physically, analysts will better be able to understand *detailed* policy needs and anticipate what kind of intelligence policy makers may need in the future.

In such a future construct, managers will function less as intermediaries who control the information flow to and from policy makers. Instead, they will become facilitators who monitor the dialogue between policy makers and substantive experts to ensure that Community resources are appropriately allocated to priority tasks and to help say "no" to requests when resources are not available. Managers also would perform the vital function of ensuring that intelligence does not become politicized as a result of the close analyst-policy maker working relationship. Indeed, if the system functions correctly, analysts and collectors, with some guidance from upper management, should be able to respond quickly and objectively to policy maker needs and be able to anticipate future needs that policy makers have not yet articulated. However, if the Intelligence Community does not take advantage of technological developments and reduce bureaucratic barriers, it will fail to meet its basic mission of providing policy makers with timely, objective, and useful intelligence.

COLLECTION SYNERGY

Executive Summary

This study addresses how efficiently our collectors work together ("synergy"), the budgetary balance between collection and "downstream" activities, and ways to reduce collection costs, primarily in the satellite area.

Regarding collection synergy, the study concludes that we are only beginning to look at how different forms of technical, human and open collection could be developed, budgeted and operated to work together cohesively and efficiently. If we proceed as now planned, progress will be very slow. Recommendations, therefore, include opting for a "revolutionary" rather than evolutionary approach. We should develop technical work-arounds for existing systems, and through an independent body establish as soon as possible the common standards and protocols to provide for intra- and cross-INT interoperability, based as much as possible on commercial standards. There should be much greater attention to cross-cueing our collection through integrated collection management using improved, common data bases. We must also better manage the balance between crisis and longer-term target priorities.

Since the fall of the Berlin Wall and despite the exploitation and dissemination problems revealed during the Gulf War, collection, especially satellite-based collection, is taking an increasing share of the budget. We should be shifting more money into processing, exploitation/analysis and dissemination. This is possible without sacrificing collection capability and even as we make greater efforts to overcome denial and deception, because technology and streamlining offer the potential for large cost savings. Numerous areas, other than synergy, where we could reduce collection costs are listed, and study of the feasibility of a "market" approach to collection budgeting is suggested.

COLLECTION SYNERGY

Scope

This paper is weighted toward satellite collection issues, although it addresses the interaction between satellite, aircraft and other collectors.

Issue Summary

There is no doubt that U.S. intelligence collection capability far surpasses that of any other country, particularly with respect to technical collection, and that this capability has been the envy of both allies and enemies. Questions regarding collection have focused on whether we could sustain and improve collection capability at greater efficiency and lesser cost, and whether existing trends should be maintained or altered in order to preserve the US collection advantage for the future.

The following have been identified as problem areas relating to collection, and will be discussed further in subsequent sections of this paper:

1) Collection management lacks the accessibility, flexibility and dynamism necessary for the post-Cold War period. At present there is an imbalance in collection management priorities favoring near-term crises at the expense of baseline capabilities and future needs. The erosion of regional data bases is expected to accelerate as limited assets are focused mainly on a relatively few top Presidential Decision Directive - 35 (PDD-35) priorities.

2) Collectors work independently and thus at suboptimal efficiency, in separate "stovepipes."

3) There appears to be an imbalance between collection and "downstream" capabilities, especially in projections of the future; regardless, it appears that significant savings could be made in satellite collection without sacrificing capability.

4) The Intelligence Community (IC) appears unable or unwilling to make cross-program, cross-INT budget tradeoffs. Budget priorities and cuts often are not driven by requirements/users. The division of resources between the "INTs" is largely static.

5) Proponents find greater difficulty in funding relatively inexpensive collectors/technology than in funding high-cost programs.

6) Spacecraft and associated systems are becoming ever more costly and consuming more of the intelligence budget.

7) We need more, rather than fewer, spacecraft platforms for better global coverage, more frequent revisit and reduced vulnerability. Demand outstrips capability. Denial and deception problems are increasing and the planned future architecture makes us more vulnerable to them.

8) There are very long lag times in getting technology on orbit. We need to adapt to commercial standards, technology and processes.

9) Unrealistically low spacecraft life calculations exacerbate problems of cost, fielding timely technology and maintaining the industrial base.

"Synergistic" or "Fused" Collection

At present, collection platforms normally are "stovepiped" to operate independently from other collectors, including completely distinct processing systems, and usually unique exploitation, dissemination and receive systems as well. While in the best cases a coherent "end to end" system is created, usually this involves considerable inefficiencies in collection tasking, and in achieving an "all source" intelligence picture that meets user requirements and that gets to the deployed military user in a timely way.

Synergistic or fused collection would make more efficient use of collection assets through timely tipoff, cooperative geolocation, avoidance of duplication, assignment of the most efficient collector for a given task, and through coordinated orbits or collection plans. There seems no doubt that collection assets could work together far more efficiently had they been deliberately designed to do so. However, continual technology advances in key areas also present much greater opportunities for end-to-end synergy than existed previously: broadband communications, data compression, large data base methodologies and data exploitation tools all allow broadened opportunity.

Technical and other collection assets could be employed cooperatively rather than independently, tipping off each other with minimal time lags. The aim should be to achieve greater efficiencies and higher quality product through coordinated collection, so that the total product when collectors are working together is greater than would be the sum of their output working separately, as they do today. Such efficiencies might also reduce costs by allowing deployment of fewer collectors to achieve given requirements.

It should be possible, for instance, to avoid redundant collection and to select the most effective and least costly collector. Cross-tipoff or "cross-cueing" of technical platforms would allow near-real-time reaction to overcome denial and deception tactics or to capitalize on opportunities. Likewise, key human intelligence (HUMINT) or open-source data should be distributed and rapidly acted upon by other collectors. Coordinated use of satellites and of aircraft-satellite combinations could permit greatly improved tasking and geolocation without deploying additional platforms. During crisis or war, efficient use of collectors becomes particularly important, because there is great competition for limited assets.

Historically, very little attention has been accorded to synergy in the collection area. This is partly because each of the INTs developed in its own "stovepipe," with jealous protection of bureaucratic turf. Even within agencies, there was very little cross-cooperation between program managers. Rivalry among National Reconnaissance Office (NRO) components and program managers was legendary. Aircraft and spacecraft architectures usually were developed separately, and service rivalry impeded comprehensive aircraft planning or division of labor. Tasking of and reporting from sensitive CIA/Directorate of Operations (DO) human assets is highly compartmented, as are the existence and operation of other "black" collection programs and many of the sources managed by the National Security Agency (NSA). Open source information often was slighted or belated, and is distributed in separate unclassified channels.

The habit of operating in isolation extends from collection through distribution, each INT or program often having developed its own idiosyncratic communication and receive system. As a result, the systems and their collection managers usually cannot "talk" to each other for rapid tipoff or cooperative target geolocation (especially important to overcome denial and deception and in wartime). Individual users receive directly only the data for which they have procured specific receive equipment, if indeed the communications capacity is available to distribute that data. Just as we have had difficulty getting data collected by national systems out to the field, often we are unable to transmit collection from tactical assets back to the United States, where it could be integrated with data from other sources and evaluated by more analysts.

There have been some initial steps to address these problems, but most are in their infancy. Not only is there a very long way to go, but we should squarely face the choices between fragmented and comprehensive, as well as evolutionary and revolutionary, approaches. Maintenance of adequate security represents another challenge.

Fused collection is particularly difficult in the signals intelligence (SIGINT) world, especially when it is to be utilized for geolocation purposes, because collectors operating at vast distances from each other must determine whether they are receiving

the same signal at the same precise given time. One of the major impediments to this is synchronizing (signal) time of arrival to a specific portion of a single SIGINT electromagnetic wave. This, in turn, requires that each collector be synchronized to precisely the same "clock" in nanoseconds, to determine the precise receiver location -- a feat difficult in itself, but even harder when each system was developed independently with varying precisions, equipment and methodologies. Ongoing R&D is addressing the timing problem. Even if it is solved, a means of communicating the data between collectors, especially when field-deployed or mobile units are involved, can be a formidable task. And if the communications lines exist, efficient operation requires that data formats be compatible, again problematic when each of the existing systems was developed in isolation.

The Defense Airborne Reconnaissance Office's (DARO) Joint Airborne SIGINT Architecture (JASA) attempts to evolve standards, interface protocols, hardware and software to develop coordinated and interoperable airborne SIGINT collectors.

The apparently large disconnect between the spacecraft and aircraft architectures should be a matter of high-level concern. The NRO and DARO have executed a memorandum of understanding which provides for common standards, especially in timing clocks. However, in other areas, spacecraft and aircraft will continue to go their separate ways unless further action is taken. Distribution systems, data formats and data bases will not necessarily be interoperable. Each community will develop its own software, although much of this probably could be shared. Developmental work on attacking the most difficult existing and future signals should be better integrated between spaceborne, airborne and ground systems.

Indeed, it often appears that cooperative focus on improving performance in core present and future SIGINT competencies has taken a back seat to one of the more difficult and even exotic SIGINT applications, i.e. extremely precise target geolocation. The latter has been driven by the military development of expensive precision-guided weapons which often outstripped the ability of US intelligence to provide highly accurate target positions. In the process, more basic concerns -- such as the less difficult but potentially very productive task of rapid tipoff between collectors and the issue of whether we will even be able to find future signals in order to geolocate them cooperatively -- appear to have been given less priority for collaborative effort. It is also unclear whether the NRO will, in practice, accord increased synergy the priority it has received historically.

SIGINT has captured most of the attention regarding synergistic collection, and the reason for this is unclear. Imagery requires less precision and overall, is easier to "fuse." Further, while the NRO likes to advertise its goal of creating a "system of systems," cross-INT collection synergy does not seem to be receiving much attention.

As other studies have pointed out, at present there is no structured, consistent Community-wide set of requirements for the collection, processing, exploitation and dissemination of information. Processing includes storage, translation, scanning, formatting, structuring, indexing, cataloging, categorizing and extracting; there are no Community standards in any of these steps. Therefore, tasking systems also must be "stovepiped" according to the platform or the "INT." Archived material must be retrieved through varying procedures, and in some cases, archive retrieval nonetheless has been extremely inefficient. If we could achieve a single workstation for exploitation of all INTs, we could much more easily serve the user, address gaps in the data bases and requirements, evaluate information sources and task collectors.

In theory, there seems no reason why this cannot happen. With the move to digitization, "bits are bits," and data consists only of ones and zeros. With coordinated and accepted standards and protocols, compatible automated systems could be built which would be able to exchange data. If these standards and protocols were made as close as possible to commercial standards, various users not only would enjoy independence and flexibility in selection of vendors, but also would experience considerable cost savings both at the outset and for upgrades.

Examples such as the cable companies' expansion into various forms of data transmission should be an inspiration for the IC and a partial basis for judging its efforts. Cable companies now are creating systems to accommodate video (IMINT), telephone and fax (COMINT) and computer exchanges. But the revolutions witnessed in the commercial world have been slow transferring to US Intelligence, which will increasingly lag unless it opts immediately for a much more vigorous, ambitious and holistic approach. Further, the problems experienced recently with Joint Deployable Intelligence Support System (JDISS) indicate that serious follow-up enforcement must be part of the plan.

Collection Management

It has been argued above that collection platforms should be built and operated to function in complementary and coordinated ways, to improve efficiency. Many of the barriers to this goal are cultural, political and institutional rather than technical. At present, each service or "stovepipe" controls its own collectors, subject to the direction of standing requirements committees or, in crisis and war, to the overriding authority of the Joint Task Force Commander or his designee.

The Persian Gulf War illustrated the difficulty of achieving centralized control even when one has the putative authority. Theater collection managers found it hard to ascertain what assets were in theater, much less to control them intelligently. With the eventual availability of over 150 types of platforms of varying capability, it was extremely difficult to find anyone with the requisite knowledge to orchestrate them effectively.

Military service specialties do not include intelligence collection management, and relatively few analysts take the time to learn the arcane technology and requirements processes. When overwhelmed with duties, one of the first tasks they eliminate is collection management; and if they are assigned to a low priority area, this increasingly is a practical decision, since their submitted requirements often are unlikely to be filled anyway. There are not established lists of people with such competency, so reliance is placed upon a word-of-mouth "old boy" network to find and reassign known experts. As a result of these deficiencies, national collection management experts had to be seconded to the theater, departing at a time when their skills also were most needed at home.

The Gulf War allowed a six-month buildup, which was fortunate, because from the intelligence collection viewpoint, the time cushion was desperately needed. Less than 50 intelligence experts initially were allowed in theater. Weapons also were given priority over intelligence collection platforms, in the view that this would best deter the Iraqis from hostile action. Even when intelligence platforms could be imported, those controlling them sometimes were uncooperative, the classic case being Air Force policy regarding the developmental Joint Surveillance Target Acquisition Radar System (JSTARS) aircraft. Jointness and cooperation were enforced by placing intelligence experts from different venues side-by-side with each other and with operators, to overcome historical barriers to cooperation. Deconfliction of requirements became a delicate assignment, for instance sorting out the Army and Marine desire to focus JSTARS on moving targets across their lines and the Air Force demand for focus on deep strike targets for the air campaign.

With requirements far exceeding capabilities, collection managers sought to utilize non-traditional sensors, which sometimes could be useful for tactical reconnaissance. They had great difficulty finding out about these sensor capabilities and then in finding out where these systems were deployed on the battlefield. Even five years later, an inventory of such supplemental sensor capabilities apparently has not been made.

At the national level, collection management has become increasingly contentious, even before the number of satellites on orbit is slashed within the future architecture.

With requirements always far exceeding collection capabilities, some argue that program managers are largely free to pick and choose which targets they will pursue. These targets, it is said, often are those that will make their own INT's performance look good and give them visibility in the crisis of the day. They are not necessarily those that are the most difficult "enduring challenges" or those most uniquely accessible by their particular "INT" or collection system, it is argued, and indeed, they may not know what others are collecting, especially in the case of highly compartmented HUMINT or technical programs. The current system is criticized

because the stovepipes essentially control their own budget size and allocations within that budget, although in reality they have little idea how their requirements and capabilities should be prioritized compared to others. And finally, the program managers write their own "report card", with little oversight or review by others.

A persuasive argument can be made that the best potential requirements and collection managers are not the program managers or INT-based requirements committees, but rather all-source analysts with expertise in the specific mission areas who have access to all associated collection compartments and data. Some argue that not only should such analysts be responsible for day-to-day collection management, but also that they should have more say in allocating funds for new collection platforms. Taking this last point further, some believe it would be useful to give such issue managers discretionary funds to develop relatively inexpensive collection techniques to fill gaps in their respective areas. On the collection management side, the Counterproliferation Center (CPC) has negotiated agreements whereby some of the INTs have passed much tasking responsibility to the CPC; the result is said to be improved collection and a reduced need for duplicative analytic capability within the INTs, plus a freeing of the program managers from this onus, so they can concentrate on other responsibilities.

A contrary view recently was presented by the Intelligence Capabilities Task Force, however, which found a high degree of agreement between analysts and collectors that somehow system program managers left to their own devices have managed to build the right system and collect the right material. The Task Force does concede that there exist many "enduring challenges" or gaps, as well as a growing denial and deception problem which has not been acknowledged by most analysts.

Just as there is often little control over disparate theater operations unless a Commander-in-Chief (CINC) effectively exercises his options during crisis, at the national level there is no centralized collection management looking across all the INTs and deciding which can most effectively pursue a given target. This deficit arguably has become more problematic since the end of the Cold War. The Soviet targets on which most of our collection previously was focused were largely predictable and slow to change. Most US intelligence players had a fairly set role, and relatively infrequent differences at the margins were adjudicated at a high level rather than on a daily working basis. Now, however, targets are dispersed worldwide and far less predictable, and the strain on resources is greater. Yet we tend still to concentrate on management of static target decks, even as the need grows for far more flexible, *ad hoc*, rapid reaction to changing circumstances and opportunities -- for support of the military balanced against enduring requirements; for overcoming denial and deception, and for effecting synergy through rapid response to tipoff.

The new strain on collection management is especially exemplified by the dilemmas arising from the recent development of simultaneous military involvements

in various areas of the globe. Partly because US political culture has evolved to intolerance for even a low level of casualties, military and political leaders are inclined to throw all available intelligence resources against these sensitive situations, even though their marginal contribution there may be far less than if they were collecting in a non-crisis area. Hence the foundation of the widespread complaint among top civilian analysts that collection has been excessively skewed to support for current military operations, to the fundamental detriment of maintaining an intelligence base on non-crisis areas and issues more fundamental to long-term U.S. security.

While support for military operations (SMO) is seen as the culprit, however, in reality this is not a "national versus military" dichotomy, but rather a near-term or crisis focus at the expense of medium- to long-term requirements, the latter including SMO. This is true for two reasons: first, the top "national" leadership and users are clamoring for crisis coverage as much as is the military leadership, since military involvement and setbacks in such spots have considerable political as well as military implications. Second, those areas from which collection has been drawn off are also extremely important to the military. Indeed, since military interventions have been occurring in unpredicted areas of the Third World, failure to maintain an adequate base probably will affect most severely our future capability to support military operations.

When requirements outstrip capability, prioritization obviously is needed. However, PDD-35, which established a "tier" system for U.S. Intelligence, in some ways appears to have worsened the problem. Analysts believe the tier system is being imposed too rigidly. As a result, the top five or six requirements receive the great majority of the resources so that we do them exceedingly well, but those below, especially those beneath the top tier level, languish with leftovers at best.

While this would not become a major issue if intensive intelligence support for interventions or crises lasted only for a few months, prolonged involvements have become increasingly common and have intensified collection management conflicts. Critics of such diversions argue that decisions such as these often have reflected a lack of appreciation for balancing requirements, for longer-term US priorities and needs, and for the fact that piling on additional collection may bring only marginal value added, but at considerable opportunity cost.

Such acrimony can only be expected to increase dramatically in the future, if we implement plans to reduce greatly the number of satellite collectors. And the accumulation of diverse capabilities on huge satellites means that whatever such a satellite's theoretical collection capabilities, in reality, severe tasking conflicts often will develop; pursuit of one task may have to be accomplished by excluding use of another capability, or the attempt to execute both over a given area and time may cause inefficiencies.

What Share for Collection ?

During the 1980s, critics argued that US intelligence had a largely peacetime orientation toward arms control and other "national" issues, and that it was not designed to serve the warfighter well. With an orientation on collection and a focus on distribution to national users located primarily within the Washington beltway, it did not demonstrate the agility, rapid data fusion or dissemination to far-flung areas which was needed to support field operations efficiently. Although the Gulf war was a far less stressing scenario than we might one day face, and although US intelligence performed well overall, the legitimacy of these critiques largely was confirmed in 1990-1991.

The need for more investment in processing and exploitation has deepened as collectors are being designed to amass far larger volumes of data.

Critics also long have contended that expensive satellites are not being used efficiently, especially during the early deployment phase of new and upgraded systems, because requisite processing and exploitation capability on the ground are given short shrift and developed only belatedly and sometimes halfheartedly. As a result, billions of dollars routinely are spent on collection systems that have for long periods of time been used suboptimally.

The data available to date have indicated that the tendency to favor collection has grown stronger rather than weaker. Since 1992, the budgetary priority and dominance of collection apparently has increased rather than decreased. As the intelligence budget has declined, collection has taken fewer cuts within both Tactical Intelligence and Related Activities (TIARA) and National Foreign Intelligence Program (NFIP) budgets, and hence consumes a larger share of available resources than previously.

The NFIP collection budget is dominated by the National Reconnaissance Office, whose budget has climbed fairly steadily and is projected to continue doing so. The requested National Reconnaissance Program (NRP) share of the NFIP, therefore should continue to rise within a static or declining overall NFIP budget. Satellites and associated ground facilities also were taking more of the reduced collection portion of NFIP funds. Nonetheless, the overall collection budget has been faring better than other portions of the NFIP. The TIARA budget is weighted less toward collection, probably in part because many intelligence dissemination systems must be financed within the services. Comparison of 1989-91 figures with 1995-97 projections also show that collection has fared well within TIARA.

With respect to TIARA, it should also be noted that unmanned aerial vehicles currently developed as prototypes under Advanced Concept Technology Demonstration (ACTD) programs are not funded for production, and collection budget

increments for this purpose might be necessary beginning in FY 1998-2000. Likewise, there is a potentially large unfunded processing, exploitation and dissemination bill for these systems; attention and funding to date usually has concentrated on the collection portion, despite historical neglect and inadequacies in other areas. Overall, TIARA investment in imagery collection has been increasing, but imagery processing and dissemination admittedly are not funded adequately under current TIARA projections.

Many in both the Executive Branch and Congress, including this Committee, increasingly have objected to the traditional budgetary dominance of collection and believe we could achieve more value for the marginal dollar by shifting funds to processing, exploitation, analysis and dissemination. This consensus has grown since DESERT SHIELD/DESERT STORM highlighted deficiencies in "downstream" activities, notably dissemination. The aforementioned Intelligence Capabilities Task Force also has provided a dissenting note on this issue, however, finding that collection and production/analytical capabilities have been pretty well balanced, and that if anything a slightly greater emphasis on collection may be needed. It should be noted, however, that at present we often collect significantly less than our capability, since platforms are built with capacity excess to projected normal operating requirements to allow for surge capacity.

Regardless whether collection and downstream capabilities other than dissemination were well balanced in the past, many would argue that there will be a future imbalance favoring collection if action is not taken. They fear that it will be difficult to make efficient use of large prospective increases in data, to be collected by technical platforms now planned or under development as well as by "open source" methods. Indeed, some top analysts believe the community already fails to exploit adequately the imagery and signals data currently being collected and processed. While inevitably we will always collect significantly more data than we use, some wonder whether we can continue to explain or rationalize the collection of large excesses, especially since only a very small part of what is collected is actionable. Prominent experts have voiced to the Committee worries that in the future it will become more difficult to separate the wheat from the chaff, and that we could become overwhelmed with data and unable to reduce it to the information we really need. Some have wondered whether we will need a new class of data sorters, to cull information to forward to data users.

On the other hand, however, users -- and builders -- sometimes have been loathe to reduce collection platform requirements, which might in turn reduce costs. Some also note that arguments over intelligence assessments usually are resolved definitively only by acquiring more data, not by more analysis.

The Chairman of the House Permanent Select Committee on Intelligence (HPSCI) has adopted a position that fundamentally transcends this argument about

whether there is an imbalance between collection and downstream activities. It is his view that satellite collection and ground systems, which as noted above account for approximately half the NFIP collection budget, probably could be accomplished for far less money, thus freeing up large sums of money for more innovative collection schemes, for greater investment in downstream activities, and/or for reductions to the intelligence budget. This reduces us to the proposition that we can do it smarter, that technology allows the future NRP to collect as much as or more than now planned, for much less expenditure. The aim should be to reduce substantially the cost of some or most "baseline" NRO systems in order to free up money for other purposes. Moreover, we should attempt simultaneously to decrease satellite system vulnerability and increase our capability to counter denial and deception.

In its FY 96 authorization bill, the Committee advocated immediate and aggressive development of prototype small spacecraft imagery alternatives, including associated rapid acquisition practices and perhaps completely modernized ground facilities. The authorization conference referred this proposal to an independent panel established by the Director of Central Intelligence, which is to report back this spring.

Potential savings could contribute greatly to containment of collection costs, with the added benefit of providing more platforms, thus decreased vulnerability and greater coverage or revisit. While small satellite applications have to date concentrated on imagery platforms, their potential for SIGINT and communications applications also should be accorded high priority. Regardless whether the panel decides to proceed with development now, we believe that smaller and cheaper satellites are the technological wave of the future, and that the IC also will adopt them eventually, if belatedly. Secondly, the Committee initiative already has spurred the admission that far lighter and less expensive "medium satellites" could be built, confirming our view that considerable reductions could be made to the NRP spacecraft budget. To date, there has been less study and movement regarding ground systems.

Thus far, the NRO's reaction to rising costs has been the opposite of what we have recommended. Acknowledging that space system costs were becoming prohibitively expensive, the NRO accepted the recommendations of a 1992 panel to reduce the number of spacecraft on orbit by nearly half, compensating for this by loading up still more investment and capabilities on the remaining upgraded platforms. The theory behind this was that after initial investments, constellation costs would come down. Instead, however, it appears that, at best, expenditures would level out at higher levels that previously. In effect, we have roughly doubled our costs per spacecraft, as well as increasing our vulnerability to denial and deception and to accident or attack.

Technology Allows More Capability at Less Cost

Two Committee *IC21* hearings on technology trends reinforce our conclusion that commercial technology and practices hold the key to relatively painless reductions in collection costs. Witnesses agreed that commercial technology is much cheaper, is widely available, leads government R&D in many areas, and is characterized by rapid (six to 24 month) generational turnover. The challenge for government, they said, will be to concentrate government R&D in key niche areas with little commercial use or interest, and to change radically our acquisition philosophy and processes. Success will be dictated by our ability to concentrate on swift application and fielding of commercial standards and the latest commercial technology, allowing us to maintain a qualitative and cost advantage over adversaries. This will also permit a more robust, competitive and easily maintained industrial base.

Of all the technology advances, perhaps the most important is in processing and microelectronics, or "information technology." Rapid generational advances in this area, with turnover every six to 18 months, have important applications throughout the intelligence spectrum, from "upstream" collection through "downstream" processing, exploitation and dissemination.

These continuing revolutions in processing capability, for instance, help permit fielding of spacecraft that are not only lighter and cheaper but also smarter, allowing greater on-board processing of information. The latter, in turn, could permit direct dissemination to the field and communication between satellites. For some applications, eventually "micro-satellites" deployed in "clouds" and communicating with each other and possibly with a larger mother satellite might feature distributed collection and division of labor, thus allowing inexpensive reconstitution or selective parts replacement.

Rather than embracing the advancing technology, however, the NRO opted to continue making very large satellites, which are very costly in themselves and also are extremely expensive to launch. Partly, these decisions traced to an assumption that we could not get all intelligence assets off the TITAN IV, and if we could not do so, we might as well put a lot of NRO spacecraft on TITAN IV in order to avoid increasing the already enormous costs per launch.

Therefore, for example, despite major advances in composites and lightweight materials, spacecraft bus often remain very heavy. Similarly, electronics often are much heavier than current technology allows. Examples of major technology advances which could be incorporated to reduce spacecraft size and cost while retaining capability include: gimballed or phased array antennae; high efficiency solar arrays and high density batteries; high performance computers and digital commercial DRAMs; and more advanced attitude control systems such as Inertial Measurement Units (IMUs), Star Trackers and Global Positioning System (GPS) receivers. Even

where the NRO has pioneered new technology, its baseline programs have not always moved to put it on orbit quickly.

In processing, too, better adaptation to commercial standards and rapid technology advances should revolutionize the way the NRO and others do business. In the NRO, ground processing policy often has mirrored the approach to associated satellites. Usually we have resorted to very expensive upgrades of custom-built, vendor-specific, old and inefficient technology. This is one reason why ground processing now can represent two-thirds of space system costs. With dramatically improved processing power and software based as much as possible on commercial standards, tremendous efficiencies and cost savings are possible. This is why some of the small satellite proposals advocate redesigning processing systems with "a clean sheet of paper" approach. Because individual satellite programs currently use different contractors with system- and proprietary-unique processing, this must be changed before we can fully acquire cross-platform, cross-INT collection synergy. This also reinforces the need to integrate ground facilities based on common standards and protocols and on commercial technology to the fullest extent possible.

Smaller satellites could potentially feature life cycle costs less than half those of some current satellites, freeing up billions of dollars. Often, smaller satellites also offer important advantages other than financial savings; one major point is that we could put more platforms on orbit, allowing better revisit time, more flexible worldwide coverage, decreased vulnerability and more a efficient industrial base.

Advanced technologies such as those allowing increased processing aboard even lighter weight spacecraft now render it possible to disseminate selected data direct from the satellite to simplified, distributed ground stations. This might gratify users by sending some data directly to the field, and it could also reduce our vulnerabilities due to chokepoints in these systems. And, once again, it is commercial technology which has led the way in developing concepts for direct dissemination to individual users.

There has developed a belief that "direct" or "global" broadcast is a better option than direct download, since it allows processing and fusion of material in the US and distribution of culled information to military units that might otherwise be overwhelmed. However, it appears that global broadcast and direct downlink (DDL) from collection platforms should be considered complementary rather than competing alternatives, so long as DDL is executed in a cost effective manner. Field ground units could collect from tactical assets and broadcast processed information up to satellites for transmission back to the US. They could task and collect from satellites via direct downlink only the most important data for their purposes, and would have only themselves to blame if they got too much to handle. DDL would ensure their timely receipt of the most important data, the ability to view high priority "raw" product fully, protection against possible communications interruptions or priority problems, and

provision of a minimum backup against satellite system vulnerabilities.

In general, this study argues that the NRO should eschew a policy of extremely expensive, evolutionary upgrades and instead seek revolutionary leapfrog technology based mostly on commercial technology wherever feasible and prudent. However, affordability also will require a change in acquisition philosophy similar to what others have urged for Department of Defense (DoD) programs. Systems will have to be produced quickly, competitively, and in larger quantities, in order to control costs and get technology on orbit promptly. DoD directives to minimize military specifications on existing and planned systems will have to be taken seriously. Management superstructure should be minimized, and personnel reduced to the minimum needed. This is contrary to current trends. Further, NRO "base" or support costs constitute fully one-third of the NRP, and have not been delineated well for outside or Congressional scrutiny.

Streamlined acquisition philosophy also focuses on requirements rather than contract specifications, allowing the contractor to determine how to meet those requirements. Fixed price contracts should replace cost plus contracts wherever feasible. In the past, NRO contractors were incentivized primarily to extend satellite life, with profits increasing accordingly. Hence, intelligence satellites have become very long-lived. This philosophy, too, probably should be reconsidered, because as technology advances ever more rapidly, it has complicated efforts to get new technology on orbit.

Despite these advances in longevity, the NRO continues to resist altering artificially low "mean mission duration" (MMD) estimates, according to which acquisition schedules are planned. The result has been inefficient procurement stretch-outs, belated cancellations, high satellite storage and team maintenance costs, constant disruption to an incorrectly sized industrial base, and attendant high overhead costs which are passed along to the government. In addition to these inefficiencies, stubborn adherence to artificially low MMDs has driven us to numerous policies that otherwise would be considered illogical, if not downright silly.

Apportioning the Collection Budget

Regardless how they are operationally used, there is widespread agreement that there is little logic in the process for deciding which collection capabilities we most need and should acquire in the first place. Not only are there few means for trading off the value of one potential platform against another, but there is little mechanism for trading off collection against other priorities.

It is striking, for instance, that the division of resources among the INTs has remained largely static over the years, especially within the NFIP, which is less volatile as a whole than is TIARA/Joint Military Intelligence Program (JMIP). This static -- or

stagnant -- status persists despite vast changes in world politics, targets, and technology.

Measurement and signatures intelligence (MASINT) also presents a perplexing case history. Difficult to understand and often without an established constituency, under the current budget allocation system, it will have a hard time coming to its own due to declining budgets. Indeed, MASINT budgets have shrunk we rushed to shut down traditional radar collectors on the theory that they no longer were needed for the post-Cold-War period. Yet many believe that MASINT collection could become the most exciting future intelligence technology if properly managed, and if these and other potential new initiatives were not considered primarily as threats to the financial viability of expensive existing programs.

Non-technical collection capabilities considered relatively cost effective sometimes also have had difficulty maintaining and increasing budget share. HUMINT, for example, sometimes has been cited as potentially far less expensive than technical platforms as a means of collecting the most highly focused and sought-after intelligence requirements, e.g., on enemy leadership and intentions. This could be particularly true if civilian and military HUMINT collectors undergo the cultural change of realizing that their future is brightest if they wholeheartedly marry HUMINT operatives to technical collection, something now made possible by the advance of technology and miniaturization.

Open source intelligence traditionally also has had a difficult time increasing market share commensurate with its potential. The growth of open source material should allow a further refinement of collection strategies and an ability to concentrate the limited number of technical collectors on the truly "hard targets." However, the burgeoning availability of open sources has complicated the IC's ability to manage the amounts of data now available. In addition, there is a bias among some in the intelligence and policy communities against open sources, stemming from the erroneous belief that no information that is valuable is likely to be easily accessible or unclassified. This prejudice severely undercuts the utility of open sources and can only be overcome through positive action. Moreover, the under-utilization of open sources -- and HUMINT -- may be due partly to a lack of understanding among users about their potential and how to use them. The IC has been addressing these problems for the past several years and should devote more resources to them, given the savings this may create in terms of overall collection costs.

Such collection budget allocation problems apparently derive partly from the observation above that each stovepipe or program determines its own budget and writes its own report card. There is little mechanism at the top level for judging between them, and some argue that it would be virtually impossible to maintain in one decision-maker or centralized location the detailed knowledge of all the diverse

intelligence programs and capabilities that would be needed to inform centralized management over a sustained period.

The only current institutional mechanism for effecting such trades within NFIP has been the Community Management Staff (CMS), which sometimes has been directed not to interfere with program managers. Moreover, program element monitors within CMS are detailed from elsewhere in the Community and eventually must return to their old positions, so are in a poor position to issue judgments which might be unpopular with their parent organizations.

Some argue that both collection management and program trades at the margins can best be effected by the all-source analysts located in centers, by task forces or by issue management teams. These persons are read into most or all relevant collection programs, know their capabilities, access and current operations, and can judge past performance and cooperation compared to other collectors.

One suggestion is that these groups be given some "seed money" of their own, so they can pursue low-cost collection programs which now languish as large, expensive programs receive the attention and money. It can be confirmed that on Capitol Hill as well, allocations of a few million dollars often are scrutinized far more carefully than large programs, although their sums amount to less than the rounding errors of the latter.

These seemingly intractable problems regarding allocation of the collection budget might be approached in a novel way by considering development of a "market" approach to apportioning collection monies, rather than the current system. The market approach would seek to avoid the problems of the "command economy" alternative most often considered; for objective, long-term expertise in these many and complex programs probably is at best fleetingly achievable in an all-powerful DCI or collection "czar" or centralized staff. A market system might also present numerous other advantages, although implementation could be difficult, at least initially. The following exemplifies the outlines of such a system, which requires further thought and development of detail.

One way in which a market system might be implemented would be to apportion among intelligence users money or monetary "chits" for the coming and out years, which they could divide and allocate among potential collection systems that appear able to meet their future requirements most cost-effectively. Those most successful in allocating their money wisely would not be punished by taking away savings, but rather would be free to use those savings for additional collection benefiting themselves.

Under this example, a method would have to be devised for fairly apportioning money or monetary "chits," representing non-baseline dollars, among

users/consumers, with flexibility for changes in perceptions of need/fairness and in national security priorities over the years. On the military side, for instance, consumers could include the Defense Intelligence Agency (DIA) all-source analysts, CINCs, services, joint staff and the Director of Military Intelligence; on the civilian side, they might include the DCI, departments and agencies, the National Security Council (NSC) and CIA all-source analysts and centers. If necessary, a means could be found to weight a portion of these votes towards "enduring challenges" or long-term gaps and for collection to overcome denial and deception, e.g., by requiring individual users suffering from such gaps to expend a percentage of their chits in this area or by setting aside a bloc of DCI and DMI chits for this purpose.

Core or "baseline" capabilities would be determined and maintained for program stability, but would be thoroughly and critically reviewed both initially and yearly thereafter for cost effectiveness and operational responsiveness to consumers. Any questions or discontent surfaced by either an independent staff permanently assigned to a CMS-style organization or by Congress and consumers would be aired thoroughly and periodically reviewed by the consumers, with budgetary adjustments made accordingly.

An accumulation of enough "chits" could either finance a fully designed and costed system as presented to users or, in planning and requirements stages, represent the cost and requirements/users for which a system should be designed. Program managers would have to market their proposed product among potential users/payers/voters. A truly independent CMS (not using agency detailees) could serve not as the DCI's resource to grade and prioritize programs, but as a "truth in marketing" organization for technology risk and cost estimates, to which users could refer (cf. *Intelligence Community Management* staff study). If high-cost but necessary systems could not achieve funding "critical mass," a "runoff" system might have to be developed.

Such a "market" system would appear to have the advantages of: naturally eliminating unnecessary redundancy; favoring lower cost systems; forcing users to prioritize their requirements more carefully, since users would have only a limited amount of money to spend for their particular needs and would be truly paying the bill; forcing a debate over requirements priorities, both when distributing and when expending chits; and presenting incentives for cross-service, cross-TIARA/JMIP/NFIP investments, depending upon which option would meet needs at lowest cost, since the user would be able to retain savings for other purposes. Program managers would be incentivized to minimize compartmentation and program costs, and both they and users would be motivated to form groups of multiple users who might share the bill. Once the system was operational, collection management would be geared to satisfy those who had paid the bills, in order to sustain their support for the existing system and maintain consumer trust for future budget decisions; utilization for other unforeseen customers could be directed by the DCI or his collection deputy. As in a

true market system, the DCI and other users would be free to trade informally some of their own chits/votes, as they saw fit.

The system would become more free-wheeling, and aspects of it might seem undesirable to some. Consumers would have to become far more educated on the range of collection systems and opportunities than most are now, and inevitably would make some errors. Political infighting and wheeler-dealing would continue to flourish, especially over consumer "chit" allocations. Expert marketing or salesmanship could become a program commodity as valued as substantive expertise. However, consumers primarily voting their own self-interest ultimately should produce a more rational, efficient, fair and flexible system than we have now or than could be achieved and maintained under "command economies" overseen by the DCI/CMS, DMI and individual services.

Recommendations

Collection Synergy and Collection Management

1) Interoperability should be effected through a high-priority **revolutionary approach rather than through the evolutionary methods now contemplated;** the latter would delay achievement of extensive synergy for a generation. This revolutionary approach would accept more short-term risk and disruption in exchange for much larger and quicker pay-off.

- For the **near term, universal translators** should be developed and fielded to put headers on data coming from "legacy" collectors using diverse protocols and standards, thus providing a conversion factor for all pulse description words.

- Over the next five years or so, **comprehensive standards and protocols** (for timing, ephemerus, frequency, geodesy, etc.) should be developed and enforced for new systems, similar to the multi-layered standards set for the computer science industry by an international standards organization.

- Synergy thus should be maximized from collection through processing, exploitation and dissemination. The number of unique systems and components should be minimized, and use of commercial off the shelf components maximized. With digitization and proper standards, we should eventually be able to disseminate, exchange and exploit all data within a common transmission/receive system, just as the commercial world now is leading the way in routing voice, video, computer and fax over the same lines.

2) **An independent DCI/Secretary of Defense (SECDEF) level board should be established which sets and enforces all necessary standards, protocols, etc., for intra- and cross-INT interoperability from collection through dissemination and exploitation, basing them as much as possible on commercial standards.** (cf. *Intelligence Community Management* staff study and its discussion of the Infrastructure Support Office (ISO)).

3) **While we should be effecting a shift from single system geolocation to collaborative geolocation, too much of the initial focus of fused collection has been on what might be the most demanding of fusion problems, i.e., the achievement of extremely precise geolocations. Much greater effort should be devoted now to cross-cueing and integrated collection management, with high priority on cross-INT aspects.**

4) **All-source analysts extensively trained in collection management and with access to data from all collectors relevant to their mission area should select and task the collectors most suited to their problems.** (cf. *Intelligence Community Management* staff study on CMS collection management and electronic connections with analysts and collectors.) A concerted effort must be made to develop and sustain this expertise at both the national and tactical levels, through **improved, centralized cross-INT collection management training and utilization programs.**

5) It seems necessary to **centralize collection management** in order to: reduce duplication; effect cross-INT trades and use the most efficient collectors; achieve desired collection synergy and counter-denial and deception (D&D) capability; and provide improved collection dexterity and responsiveness suited to the post-cold war world. (cf. *Intelligence Community Management* staff study.)

- With improved communications and computer programming and graphics, and with a transformation to "bits are bits" synergism, **multiple centers** could exist with independent capability and full interoperability. For instance, there could be a national collection management center as well as tactical command and control/information centers in each major regional command, plus *ad hoc* hoc teams for local crises or operations.

- **Computer programs** could depict all available assets and their tracks, and automatically compute the most accessible and cost-effective collection solutions. Interoperable dissemination could bring all requested data from any source down to a single point -- with digitization, "bits are bits."

6) **Improved, common data bases with easy retrieval by those at remote locations** are essential for synergism in both tasking and exploitation. (cf. *Intelligence Community Management* staff study.)

7) The Intelligence Community must **find a better way to manage and balance near- and longer-term priorities, which recently have become too weighted toward support for current crises and interventions.**

Collection-Downstream Balance

8) **The NFIP/TIARA budget should be broken out within the five cross-program categories of collection, processing, exploitation/analysis, communications/dissemination and infrastructure.** The purpose of these groupings would be to focus policy and budgetary attention on the relationships and trends between the five components. At minimum, overall figures with accompanying tables of component line items should be presented in overview books/portions of the Congressional Budget Justification Books (CBJBs)/Congressional Justification Books (CJBs) for FY 98 and beyond. This approach could be compatible with and complementary to mission-based budgeting. If detailed mission based budgeting does not prove practicable, these five divisions could form the basis for building the budget and for organization of all CJBs/CBJBs, and could be a vehicle for forcing competition for decreasing funds within and between the five divisions. Categorizing the budget in this way should also incentivize programs to reduce costs (see below).

- The collection category should include the platform command and control portion of the ground infrastructure, but there should be further study of whether any initial ground processing should be included within the collection category, and, if so, to what level.

- **TIARA, JMIP and NFIP activities should be budgeted and operated cohesively**, since the distinctions between them are decreasing or disappearing.

- **Congressional budgetary oversight** would best be organized along these five budget categories as well.

9) **The DCI and Secretary of Defense should determine percentage allocation goals among these five components, which would redistribute resources over a defined period of years to a more rational and less collection-heavy budget.**

- **Exploitation/analysis should receive highest priority** for improvements, especially automated exploitation/data screening; an attempt should be made to **quantify the extent to which automated exploitation improvements are needed** to cope with increased data flow and to quantify how increases in collected and processed data and improvements in automated exploitation should affect analytic manpower levels. **Dissemination** also is a very high priority, but more rational, cross-INT, common dissemination of digitized information might eventually reduce funding requirements in this area. In the **processing** area, SIGINT requirements could become so financially and technically demanding that we should now reappraise the long-term cost-effectiveness and viability of current approaches. Processing should be sized and financed to ensure efficient use of new or upgraded collection systems from Initial Operating Capability (IOC) through Final Operating Capability (FOC), including in these calculations the use of likely "residual" or partially operational systems.

10) **Overcoming denial and deception** which we have experienced or to which we have known vulnerabilities **should be a major factor in establishing requirements and budgetary priorities, for both collection and downstream activities.**

- The collection community should be shifting a significant portion of its resources toward **unwarned/unexpected collection**, and downstream investment and analytical resources should be specifically devoted to means of overcoming denial and deception.

Reducing Collection Costs

11) **The following is considered a finding rather than a recommendation, which should be further studied for feasibility and implementation details. We should try to devise a system whereby all types of collection**, including TIARA/JMIP as well as NFIP, human and open-source as well as technical, **are forced to compete for money from a common, reduced pot of collection money. A "market" approach, rather than the current system or the alternative "command economy" approach, should be developed, in which intelligence users/consumers individually and collectively decide which collection systems might best meet their needs.**

12) **Costs should be delineated as thoroughly for "baseline" collection and other programs as for non-baseline programs.** The NFIP practice of maintaining an undelineated intelligence "base" should be banished, both to promote needed transparency for users and Congress, and as a logical fall-out of dividing the intelligence budget into five parts with separate lines for each, including infrastructure.

13) **Congressional Budget Justification Books** (CJBs, CBJBs) should be written to elucidate clearly the costs, limitations and mission applications of existing or proposed collection systems. If the above "market" system of budget allocations were implemented, these books would serve as the basic reference documents for users as well as for Capitol Hill in assessing individual programs.

14) **Planned NRO funding levels should be reduced, and there should be an immediate shift in direction toward rapid deployment of more, smaller and cheaper satellites** wherever this is practicable, with appropriate measures to maintain large satellites in these respective areas so long as reasonably necessary to hedge technology and development risk.

15) We should move to **supplement broad area and multispectral collection with commercial satellite sources**, maintaining a minimum core capability but relying heavily on commercial adjuncts and surge capability. Modernized ground stations should be made compatible with commercial standards and capabilities.

16) Especially if the NRO does not move toward a far more distributed, robust architecture than now is planned, the military should consider developing inexpensive and possibly reusable **"tactical satellites"** to supplement national collection over denied areas during crises.

17) **NRO ground systems should be modernized as required, using a "clean sheet of paper" approach** and employing commercially based, interoperable technology to the greatest extent practicable, except for necessary specialized applications. This should allow meaningful and continued contractor competition, drastically cut both initial and upgrade costs, and be designed to maximize synergy between collection systems and associated ground stations. A systems integrator should be hired to study the best way to effect these goals, and we should consider the possibility of maintaining updated, cohesive ground stations by contracting out to a systems integrator (cf. *Intelligence Community Management* staff study).

18) **On-board processing and partial data transfer through direct downlink** should be pursued as a means of better serving customers, reducing satellite system vulnerability and potentially reducing costs. **System vulnerability and chokepoints** should be addressed as a matter of intense concern, especially if the prospect of information warfare is taken seriously.

19) **The current method of gearing acquisition strategy to an artificially low calculation of expected satellite life should be altered to reflect actual experience and more realistic expectations. Spacecraft program managers should consider elimination of a specified mean mission duration in contract requirements and contract incentive rewards**, allowing this to remain as a "bonus" factor in evaluating contract competition.

20) **Platforms and sensors built for purposes other than intelligence collection should be used routinely for intelligence purposes** when this is possible, needed or cost effective. Sensors built for other purposes, but which might provide data useful for intelligence purposes, should be surveyed, inventoried and utilized, for both strategic and tactical collection purposes.

21) Especially in the space area, **the focus should be on technology leaps with maximum utilization of commercial developments, rather than on numerous expensive block changes and system upgrades.**

22) **The NRO's industrial base policy should be closely scrutinized.** Expenditures for this purpose should be minimized in coordination with the drive to maximize use of commercial technology. Policies for selection, especially non-competitive selection, of those companies which will survive, become "centers of excellence," or receive all future NRO business, should be revealed and externally examined for both fairness and long-term financial sense. The industrial base problems associated with building and upgrading few complex satellites with long design lifes should be examined. This approach should be weighed against the advantages and disadvantages of building many more and cheaper satellites quickly and in larger numbers, with competitive procurement of leapfrog technology for space and ground segments, rather than relying on expensive block changes and partial upgrades to old technology.

23) **A much cheaper system of reliable spacecraft launch should be developed** (cf. *Collection: Launch* staff study.)

24) **Program managers building intelligence platforms, especially spacecraft, should immediately embrace the Secretary of Defense's directive to adopt commercial standards for existing and new contracts, minimizing use of military specifications and standards.**

25) **Acquisition timelines, personnel and paperwork must be reduced considerably, to get available new technology on line rapidly and to reduce costs.**

26) **There should be a concerted effort to educate users on the utility of lower cost open source and HUMINT information, and this material (with proper safeguards for sensitive clandestine HUMINT material) should be rapidly communicable over the same dissemination system used by other collectors.**

27) The burgeoning availability of open source material presents both problems and opportunities. In order to take full advantage of open sources, **the IC must continue to develop improved means of collecting, exploiting and processing open source information.**

SIGINT: SIGNALS INTELLIGENCE

Executive Summary

The SIGINT staff study relied heavily on the foundation of the Committee's oversight and evaluation of both the National Security Agency (NSA) and the United States SIGINT System (USSS) for the past several years, to include recent hearings dedicated to SIGINT program management and the Global Network Initiative. This was augmented with two panels, one composed of the Division Chiefs within NSA's Directorate of Operations (DO), and one of the Chiefs of the Service Cryptologic Elements (SCEs); a variety of focused interviews; and a series of questions for the record.

The study states at the outset that NSA is an extremely successful organization and that the recommendations contained in the study are intended to improve an agency and a functional system that have provided invaluable support to the nation's policy makers. Although the study group does not believe that the cradle-to-grave approach to a discipline is necessarily the most constructive approach for the future, it has served the nation well in the past and certain elements of the NSA model are worthy of emulation by the rest of the technical intelligence community.

The success of the SIGINT system has been in large part due to NSA's formally established technical control over the discipline, which has resulted in the development of a coherent architecture for collection, processing, exploitation, analysis and reporting. However, this very strength has become also a weakness, as the resources required to maintain the Consolidated Cryptologic Program (CCP) infrastructure are now competing with investment in the core missions of NSA. Because of the way the Intelligence Community is structured and "managed," SIGINT requirements compete only with other SIGINT requirements within an artificial top line dictated in large part by last year's appropriated amount. Increasing personnel costs, for example, thus result in reduced research and development expenditures, one of the few "discretionary" funding categories within the CCP.

In the broadest sense, SIGINT is a "bridge" between imagery's ability to observe activity and HUMINT's ability to gauge intentions. With its current global reach and multiple sources of collection, SIGINT provides a hedge against strategic deception and can be extremely useful for the tipping of other collection assets. As the Information Age continues to evolve, the task of maintaining the SIGINT system's global reach is becoming more difficult; however, the trend towards increasingly interconnected telecommunications networks using various transmission media, in conjunction with the more fluid geopolitical environment of the post-Cold War world, makes global access more critical than ever before. Access, however, is only one piece of the puzzle. The most important challenges of the future may lie in the quantity and quality of what is being transmitted rather than the means of

transmission. The ability to filter through the huge volumes of data and to extract the information from the layers of formatting, multiplexing, compression, and transmission protocols applied to each message is the biggest challenge of the future. Increasing amounts and sophistication of encryption add another layer of complexity.

Signals Intelligence today is at a crossroads. The global revolution in communications technology demands new techniques, new procedures, and a new corporate mindset. The technical challenges currently facing the SIGINT community are daunting, but the outlook of those involved is cautiously optimistic. As with past and future SIGINT targets, the very technology that creates the difficulties can be the most effective tool to overcome them. This assumes, however, a sufficient level of investment to enable SIGINT to stay close behind technology. A commitment to preserve the technical *capability* to access and exploit all major communications media worldwide requires a level of investment that is not now planned for the SIGINT system over the Future Years Defense Program (FYDP). And yet, SIGINT is already the most expensive of the intelligence disciplines. How to balance the required level of investment in technology with the maintenance of existing core capabilities is perhaps the true challenge for SIGINT as it moves toward the 21st century.

In keeping with our recommendations in the *Intelligence Community Management* staff study, we believe that the rest of the technical collection community would benefit from the application of a variant of the DIRNSA's (Director of NSA) technical control over SIGINT. We also believe that the Intelligence Community (IC) and the nation would benefit from programming and budgeting decisions that were based on a cross-discipline analysis of collection, production and infrastructure requirements and capabilities, rather than artificial trade-offs within programs or specific disciplines. Our proposals for improved community management of R&D investment and, in particular, consolidation and reform of personnel management should also prove of significant benefit to the SIGINT community. This study highlights the need for improved management and focus of SIGINT R&D to ensure that critical areas are adequately funded and the need to reshape the workforce for the 21st century.

In a more centralized structure, the SIGINT "stovepipe" would still exist, although ideally with much greater permeability at all levels, to capitalize on the professionalism and expertise of the cryptologic workforce. However, we believe that much of the analysis that is conducted at NSA today is more properly done under the auspices of an all-source collection agency such as Defense Intelligence Agency (DIA) and Central Intelligence Agency (CIA), although this resubordination could be done electronically rather than physically. We also believe that there are specific areas of the SIGINT system that require improvement or more management attention; these are detailed in the classified study.

IMINT: IMAGERY INTELLIGENCE

Executive Summary

Imagery Intelligence (IMINT) will be a mainstay of the Intelligence Community (IC) in the 21st century. The IMINT community (IMC) today is made up of a diverse set of users including military, national, and civilian. We anticipate that the numbers and types of imagery users will continue to grow dramatically in the future, perhaps into other areas not yet imagined. Thus, it is extremely important that our imagery system be flexible to support these changing needs.

Exploitation will be the chokepoint for the imagery community. Given present trends, the number of images collected will continue to outpace our ability to analyze them. Collection costs continue to rise at the expense of processing and exploitation. Imagery analysts are working with archaic tools and the current acquisition process does not facilitate the timely infusion of new technology. This is due in part to the fragmentation of the imagery community, with infrastructure and research and development being pursued by numerous organizations with little to no coordination. Commercial imagery needs to be considered as an adjunct to national systems and plans must be put in place to facilitate its use. The IC continues to move to a dichotomy in imagery requirements: users want images in near-real-time yet also want detailed analysis. The imagery community has not yet reconciled how to satisfy these conflicting requirements concurrently. Imagery dissemination to the military below the Joint Task Force level still remains an issue and, finally, foreign denial and deception activities continue to be a problem and must be taken into account in future planning.

IMINT will see a great transformation in the next century. Commercial systems will allow everyone, including our foes, to have access to high resolution imagery. At the same time, classification of national imagery must provide the required access to allies while continuing to protect collection/processing capabilities. More cost effective collection systems are required to free up funding to support the "downstream" activities of processing and exploitation. The explosion of available imagery requires that new technologies and exploitation/production tools such as automated/assisted target recognition algorithms and digital softcopy search tools must be aggressively developed to help streamline the exploitation process. The IC must move to all-digital exploitation of imagery, with access to cross-INT databases, while progressing to a "virtual" analytic environment, and funding must be increased to accelerate the procurement of softcopy (digital) workstations for imagery analysts. Support for the National Technology Alliance should be increased to provide more flexibility in rapidly fielding new technologies and exploiting commercially available technologies. Finally, increased emphasis should be placed on spectroradiometric collection, processing and exploitation.

Thus, there is much in store for the IMC; however, it will not come for free. Funding must be increased to set up the central infrastructure needed to support the diversity of analysts, to bring those analysts the tools they need to help alleviate the exploitation chokepoint, and to increase and focus the R&D efforts to bring new technology to bear in a more rapid manner. Collection costs must be reduced so next generation systems and exploitation advances can occur. If these things do not occur, the IMC will not be able to satisfy 21st century requirements.

IMINT: Imagery Intelligence

Overview

Imagery Intelligence (IMINT) will be a mainstay of the Intelligence Community (IC) in the 21st century. The IMINT community (IMC) today is made up of a diverse set of users including military, national, and civilian. We anticipate that the numbers and types of imagery users will continue to grow dramatically in the future, perhaps into other areas not yet imagined. Thus, it is extremely important that our imagery system be flexible to support these changing needs.

The needs of the military will continue to expand, as their mission spreads into new, uncharted areas. Across all levels (strategic, theater, and tactical) we will see this new scope, in areas such as coalition operations; highly mobile, detached operations; enhanced C4I (Command, Control, Communications, Computers and Intelligence); and peacekeeping and humanitarian operations, along with further "operations other than war." These increased areas of responsibility bring with them a greater need for imagery support. Advanced, precision guided munitions will also demand a new level of sustained, highly accurate, imagery products.

Civilian and national imagery requirements will also continue to grow. We have already seen the use of national imagery spread into environmental monitoring and evaluation and aid in disaster relief, both national and international. Nevertheless, this particular intelligence source will be of primary importance for support to law enforcement, counternarcotics and counterterrorism, monitoring treaties and weapons proliferation, and strategic and economic intelligence. Again, though, there may be areas of intense, future civilian use that go unseen today, because the future availability of commercial imagery and the recent push to downgrade national imagery will potentially bring out new and different users who did not previously have access to this type of data. Consequently, our future systems must be easily adaptable in order to meet these vastly different requirements.

- **FINDING: IMINT will continue to be an important collection discipline for a wide variety of issues: indications and warning; support to the military; and monitoring arms control agreements, refugee flows, narcotics cultivation and ecological problems.**

The IMC faces several challenges and must adapt in order to maintain the level of support provided to, and expected by, today's customers in a future, changing environment. These challenges arise in almost every functional area: organization, requirements management, collection, tasking, processing, exploitation, and

dissemination. Other issues include classification levels, denial and deception, and interaction with commercial systems. Each of these areas will be addressed separately in this study.

IMINT will see a great transformation in the next century. Commercial systems will allow everyone, including our foes, to have access to high resolution imagery. At the same time, classification of national imagery must provide the required access to allies while continuing to protect collection/processing capabilities. The number of users and requirements will grow. Exploitation will be the chokepoint in the imagery process. The explosion of available imagery will overwhelm the imagery analyst unless automated/assisted target recognition algorithms or other exploitation/production tools can be developed. Spectroradiometric collection will become more important, with major impacts on the collection, processing, dissemination and exploitation arenas.

Thus, there is much in store for the IMC; however, it will not come for free. Funding must be increased to set up the central infrastructure needed to support the diversity of analysts, to bring those analysts the tools they need to help alleviate the exploitation chokepoint, and to increase and focus the R&D efforts to bring new technology to bear in a more rapid manner. Collection costs must be reduced so next generation systems and exploitation advances can occur. If these things do not occur, the IMC will not be able to satisfy 21st century requirements.

Organization

Much attention has been paid to the IMC's organization in recent months. However, great care must be taken not to break those parts that work well in an attempt to fix other perceived problems. It is obvious that the current Central Imagery Office (CIO) does not have the authority it needs to oversee a diverse imagery community. Yet, before we rush into a new organizational structure, we must ensure that this new organization, while solving immediate problems, will be flexible enough to cope with the next century's "virtual" intelligence environment.

- **FINDING: CIO does not have the required authority to oversee and effectively manage the imagery community.**

We are most concerned about a lack of CIO's authority to oversee an imagery strategic plan. Current imagery organizations are not tied together nor beholden to such a strategic plan. This results in disparate, uncoordinated allocation of funds and resources in collection, R&D, and exploitation and dissemination infrastructure. Dissemination within theater is another area that needs drastic improvement. Those areas that work well, though, are mainly within the exploitation community.

Exploitation support to the policymakers is excellent. Support to the military is also very good in the areas of strategic indications and warning, and contingency planning. However, providing adequate imagery support to on-going operations is still a challenge, and will only be more difficult in the future. Thus, it is important for any new organization to look at this picture and show how deficiencies will be improved while maintaining the strengths of the previous organizations; at the same time, this new organization must be considered within the wider context of the IC.

- **FINDING: The imagery community is badly fragmented. Infrastructure and R&D are being pursued by numerous organizations with little or no coordination. However, any restructuring should be considered only within the wider context of all other intelligence functions and activities.**

Some have suggested that a new organization be fashioned after the Signals Intelligence (SIGINT) model. Though it appears to be a convenient organizational structure, we do not believe this will solve the IMC's problems because the analogy of the National Security Agency (NSA) is not directly applicable to imagery due to major technological and operational differences in the two disciplines. We are also concerned that a major monolithic agency will be LESS responsive rather than more responsive to the customer. Finally, the risk that future imagery systems will be driven solely by technology rather than users' needs increases under these proposals (though this danger does exist with today's organizations). Some also claim that another major *raison d'etre* for this new organization is to solve the dissemination problems of DESERT STORM. We overwhelmingly agree that dissemination is a problem; however, it is hard to comprehend how an organization that has no control over theater/Joint Task Force (JTF)/Joint Intelligence Center (JIC) level forces and lower echelons will be able to solve this problem. Thus, we must again gravitate to the real problems within the IMC and focus on an organization that will be able to provide solutions to these problems.

The main problem areas we see with the current structure are imagery program management/planning, research and development (R&D), collection, processing, dissemination, and standards. A single, strong policy arm is needed for coherent end-to-end planning. Several key functions should be centralized: standards, protocols, and communications interfaces. A strong R&D oversight structure must be included to ensure that new technologies are responsive to customer requirements and that R&D funds are spent efficiently, according to an overall plan instead of each organization funding bits and pieces as is done today. The *IC21 Intelligence Community Management* staff study presents an IC that will solve these deficiencies through the needed centralization of certain functions while preserving those areas that work well.

We believe the exploitation community is one of those areas. This is an area where IMINT differs greatly from SIGINT. In the SIGINT arena, a signal is collected and analyzed by NSA, producing information which is then distributed to a variety of customers and agencies. IMINT, on the other hand, produces an image which is then sent to a variety of organizations and exploited in many diverse ways within those organizations. Hence, imagery exploiters are, in many ways, discrete customers/users of the imagery in and of themselves and, thus, the SIGINT analogy is really not applicable in this case.

Keeping imagery analysts close to their customers will become increasingly important but too great a dispersion of capabilities may lead to an erosion of imagery analysis expertise. Thus, a balance must be struck between decentralization and centralization of imagery analysis capability. Another balance that must be struck is the level of segregation between military analysts, analysts who support national and civilian customers, and cartographers. Recent recommendations have been to combine these forces into one exploitation cadre. Again, we go back to our argument that the different exploitation elements should be treated as discrete customers. There is danger in too much centralization because of the diverse sets of skills these analysts bring to the table. We fear that combining these personnel into one homogenous unit will dilute these skills into one set of "accepted" skills, which will not completely satisfy any customer's requirements. In order to preserve the diverse set of analytical skills we have today, we recommend keeping the disparate imagery analysts with their originating parent organizations, while centralizing the infrastructure that supports them; however, we also recommend better integration of the imagery analysts into those organizations for better support to the "all-source" analysts.

- RECOMMENDATION: As noted in the ***Intelligence Community Management*** staff study, **second and third-tier analysts from all INTs should be co-located with true "all-source" analysts in the CIA and DIA.**

We must look to the future, not the past, for a new organizational model. Legacy stovepipe organizations are a product of the past and will not provide the needed flexibility required to support a "virtual" intelligence community in the future. Our model of IMINT in the 21st century is based on centralization of vital functions (end-to-end planning/management, R&D, collection, processing, archiving, and infrastructure) while sustaining a diverse customer/exploitation base. Needs of the users must drive the organization and those users' needs are met mainly by imagery derived information and products prepared by professional imagery analysts, not the raw image. These decentralized production strengths equate to increased responsiveness to local needs/missions and the ability to tailor and/or focus efforts quickly to respond to changing priorities. This flexibility in exploitation, combined with

consolidation of programmatic and tasking oversight, and a standards based infrastructure, will truly allow the IMC to be responsive in the 21st century.

Requirements

Requirements on a grander scale and collection synergy are discussed in separate *IC21* studies. However, in the context of imagery, requirements and collection management must be discussed. The new Requirements Management System (RMS) for imagery is due to reach initial operating capability (IOC) in June 1996 (eighteen months behind schedule). It is unclear at this time whether RMS will be able to perform comparably to its predecessor, CAMS (COMIREX Automated Management System). In all fairness, the RMS goal was admirable: to allow the user to follow his imagery request and know exactly where it was in the requirements process. However, it is a possibility that RMS will never be able to achieve full operating capability. This is a great example of spending large sums of money on a stovepipe system. Of course, it was expected that this system would be up and running by now, and that we would be on our way to designing the collection management tool of the future. Since this is not to be, in the near-term, we must ensure that RMS will provide equivalent capability before we allow CAMS to be shut down. (Both systems cannot run simultaneously.) In the event RMS cannot meet expected performance levels, CAMS must be retained until the next generation system is available.

For that next generation system, we envision an integrated requirements process where all types of intelligence collection are tasked (e.g., SIGINT, IMINT, MASINT, etc.) Ideally, this translates into one requirements tasking system. The military's Joint Collection Management Tool, which was supposed to interface with RMS, is a small step in the right direction and provides only one interface to the process. However, this is not absolutely necessary. What is required, though, is consolidated resource planning. We must be able to do cross-platform, cross-sensor tasking, with dynamic and flexible planning, scheduling, and management. Managing which users get to steer which collection assets will be difficult. Rapid exploitation feedback will allow more optimized planning and scheduling. This all-source requirements system must be compatible with theater/tactical assets and should look to meet the goals set out by RMS, mainly that the customer would know the status of his request, for all -INTS, throughout the entire process. This is discussed in much further detail in the other staff studies mentioned above.

Validation of imagery requirements also needs an overhaul. The current Community Imagery Needs Forecast (CINF) does not currently include all requirements. It also appears that requirements are based upon what collection systems are/will be available instead of what information is required. It appears that the "Seal of

Approval" process does not address cost effectiveness or ability to fulfill requirements.

- **FINDING: The CINF is incomplete and appears to reflect only what can be collected versus what needs to be collected.**

We need a requirements system that is immune to special interests. We propose a central requirements organization that would look across all -INTs to determine the most cost-effective and capable way to collect the required information. We need an organization that looks to the future to determine which technologies require increased investments today. We would like to see the IC study and react instead of study and report. There must be thorough understanding of the problem before the IC jumps to solutions. But this should take months, not years.

- **RECOMMENDATION: As noted in the *Intelligence Community Management* staff study, a Community Management Staff with IC-wide authority over requirements, resources and collection would improve the role of all collection disciplines. This would also abet a more integrated requirements and tasking system for IMINT, which has yet to be attained.**

Collection

- **FINDING: Collection costs continue to rise at the expense of processing and exploitation.**

Only one solution has been offered so far that shows major promise in reducing costs while maintaining capabilities: small satellites (smallsats) acquired through streamlined acquisition practices. A distributed architecture made of smaller, single function satellites, will provide the flexibility and responsiveness required for the customers of the next century. Technology is now available that would allow the IC to shrink its satellite size, thus reducing costs, both for the satellite and the launch vehicle, but also from an organization infrastructure point of view. Also, by using streamlined acquisition, this approach allows new technology to get on-orbit more quickly. Multispectral sensing satellites can be added to supplement this architecture. Best commercial practices must be incorporated.

- **RECOMMENDATION: Move to an architecture of small satellites (smallsats) to increase capability, flexibility and revisit while reducing costs.**

Smallsats have also been proposed for point targets that need high resolution collection. These Narrow Field of View (NFOV) satellites, while more complex than

the Wide Field of View (WFOV), offer an exciting opportunity to maintain capability but at much reduced cost. Unfortunately, because many people believe smallsats are only capable of fulfilling narrow, niche missions, these types of satellites will never be considered seriously until this technology is proven on-orbit. (It appears that it is more widely accepted that the WFOV mission can be done than the NFOV mission). Therefore, we must build and fly a NFOV small imager to convince the skeptics that we do not need to spend billions per satellite to have equivalent capability. Thus, we must act now. As stated earlier, smallsats will not be considered as a viable alternative unless there is an on-orbit demonstration showing their worth. It is imperative that the small NFOV satellite be built as quickly as possible in order for this technology to be a serious contender.

- **RECOMMENDATION: Proceed quickly with a small satellite demonstration in order to ensure this option is considered as a viable alternative for the next generation of imagery satellites.**

Another idea that should be reviewed, especially if the cost per satellite can be contained, is to reverse the trend of increasing Mean Mission Duration (MMD) and build satellites that will last only three to four years. Costs would be further reduced, both per launch vehicle and satellite, because larger block buys of both systems would allow a cheaper unit price. Limiting the lifetime of satellites would also allow advanced technology to be incorporated more quickly and missions to be altered to adapt to new situations because satellites would be replaced at a relatively fast pace. Industrial base concerns would be alleviated and launch crews would always be current on their procedures. The recent push to increase MMD seems to be a survival tactic to counter the large growth in satellite cost; because the IC's satellites have grown so expensive, we can buy only a few, spaced out over several years. Thus, these satellites must last longer so the IC can stretch out its costly acquisitions. This approach should be given closer scrutiny.

- **FINDING: "Denial and deception" activities by foreign governments are a current problem. As U.S. imagery capabilities become more widely known, this problem will likely grow.**

Along these lines, the exploiters should be viewed as customers and as such should have input in deliberating the value of new systems because they are the ones who must use the product. They should have direct involvement in utility studies of new types of systems, which is not the currently the case. Today, the National Exploitation Lab (NEL) is only involved in these types of studies when asked to participate. They, along with all other primary users, should have the authority to demand involvement with the evaluation of any new imagery system.

The same "clean sheet" argument can be made for the command and control and ground processing segments for imagery. New commercial satellite architectures will be required to control on the order of hundreds of satellites. Can we leverage off of the work they are doing? New processing advancements are being made in the commercial sector that should be incorporated quickly. This appears to be only one of many examples where contractors have conveniently made themselves indispensable, at the expense of the government.

- **FINDING: The current imagery ground architecture is very complicated and expensive.**

Commercial companies are developing ground stations at much less cost. It gets back to the principle of deleting unnecessary layers and overlapping influences, wiping the slate clean and starting over. The IMC should look at using the "clean sheet" approach for its ground functions. It is especially important that this method be implemented now while the "lessons learned" expertise still resides within the NRO. Thus, they would have the advantage of quickly infusing new technology and simplifying operations while ensuring that mistakes of the past are not repeated.

- **RECOMMENDATION: Redesign the ground architecture from a clean sheet of paper in order to take better advantage of commercial capabilities and reduce ground station vulnerabilities.**

The NRO needs to return to streamlined program offices with smart people doing the work, thus reducing the need to rely on numerous SETA and support contractors. This, too, will reduce the costs required to procure satellites.

On the airborne side, Unmanned Aerial Vehicles (UAV) and airborne collection will continue to be important assets to support the theater and tactical commander. However, their collection capability is limited to only those areas where they can fly with impunity. However, for all airborne collection that remains, the imagery must be collected digitally in order to ensure its compatibility with future imagery databases and exploitation workstations. The tasking of these systems should be integrated with the tasking of overhead systems in order to maximize efficiency and delete duplication of collection.

Exploitation/Information Processing

Exploitation will be the chokepoint in the imagery process of the future. The amount of imagery collected will be increased greatly at a time when the number of imagery analysts will have been reduced. How to interpret new types of imagery like multispectral collection will have to be learned at a time when it will be impossible to

pull analysts off-line, unless the hiring trend for analysts is reversed. Softcopy workstations are a critical need and purchases for all imagery analysts should be accelerated. These workstations should be compatible or able to be upgraded to work with all types of intelligence and their associated databases. R&D for a softcopy search tool should be a number one priority. Either the number of analysts must be greatly increased or technology must be developed to make both the analyst workforce more efficient and to take away some of the exploitation preparation workload. We would venture that both must occur: the number of analysts must be increased and the technology must be developed, both in the forms of better workstations and better tools. R&D dollars must be consolidated in order to better serve the imagery community; however, each organization must have control over some amount of funding in order to preserve specialized tools.

- **FINDING: Given present trends, the number of images collected will continue to outpace our ability to analyze them.**

- **FINDING: Imagery analysts are working with archaic tools; the current acquisition process does not facilitate the timely infusion of new technology.**

The number of analysts needs to increase now. Also, we are facing a severe deficit down the road because of a reduction in the number of imagery analysts. The longer we wait to begin rehiring, the greater the danger we will face a gap in knowledgeable imagery exploitation. Fifty percent of DIA's imagery workforce will be eligible to retire within the next five years. This is a problem that cannot be ignored because it takes several years to train an imagery analyst to be self-sufficient.

Another problem that has occurred because of downsizing is the "in-box" mentality. This is not just a problem within the IMC but is occurring everywhere within the IC. Analysts are too busy dealing with the crises of today to have the time to think creatively and look long range. DIA, in the past, apportioned part of their personnel to look at long-term issues but they no longer have this capability. History shows that there will be problems that may take interdisciplinary teams years to solve. With the current emphasis on immediate information, there is a danger that refined, thoroughly analyzed intelligence will become a thing of the past. We must balance real-time information needs while protecting long-term research.

Another issue is the availability of analysts for the testing of new tools, products, etc. It is currently very difficult to pull analysts off-line for this purpose because there is no margin left in the number of analysts doing the day-to-day work. All of these problems hinge on the number of available analysts. Hence, we must act quickly to increase the number of imagery analysts, both national and military. The

optimum number of analysts will depend greatly on the exact mission the IMC is asked to perform and on how well we apply technology to streamlining the exploitation process for those analysts. Regardless, the number we have today is inadequate and, due to the long timelines of training, hiring of new imagery analysts should commence at once.

Future imagery analysts will face even harder tasks. They will be required to look at and evaluate diverse types of imagery and use more sophisticated tools. They will also work daily with a paradox: producing thoroughly analyzed, contextually based products while meeting demanding timeliness requirements of less than 24 hours (in some cases, 12 hours). This is an impossible task in today's environment, yet will become increasingly more important in the future as other countries gain access to similar imagery. Strategic advantage will become a matter of whose collection, exploitation and dissemination timelines are the shortest. Intelligence must be there swiftly so as to be relevant to decreasing planning and execution timelines, and packaged in such a way that can be consumed by the user. The lower echelons of the military present the real crux of the problem: extremely short timelines must be met yet great detail is still required. This would appear to be a push toward automated exploitation; this however, implies that the time-dominant reporting will not have analyst derived information and will merely report what, where and when, not who, from where and why. In some instances, this may be all that is required but it is our belief that a human will always be needed, at least during the timeframe dictated for this study, to provide the cognitive processes of exploitation. Nevertheless, R&D should be increased and focused on providing these analysts the new tools and efficient processing capability required to help them come closer to meeting these demanding timelines.

- **FINDING: The imagery community is not currently able to satisfy the requirements for both immediate and detailed analysis.**

These new tools will encompass a broad range of capabilities. In the interim, the emphasis should be on providing tools that will greatly speed up the analysts' ability to access and integrate information. Analysts need softcopy workstations that allow for timely retrieval of current and archived imagery with no degradation in quality. Softcopy exploitation will result in significant efficiencies. It will streamline the dissemination, storage and retrieval of imagery and will enhance the ability of analysts to exploit the full range of available data. It will facilitate the integration of classified, commercial and theater imagery, and will allow analysts to quickly acquire the "best" images of a target (assuming required selection algorithms are developed). The ability to perform mensuration from imagery obtained from multiple sensors at a single workstation will be a significant enhancement.

- **RECOMMENDATION: The IC should move aggressively to infuse new technologies into the IMC, such as automatic target recognition capabilities, in order to help streamline the exploitation process.**

Softcopy search of large land areas is a critical necessity yet this tool remains extremely difficult to implement. Hence, currently, it must still be done on a light table. Softcopy search tools must be developed to enable efficient search of large amounts of data. Sufficient funding in R&D in this area must be accommodated.

For the future, the best knowledge-based tools should be made available: on-line access to integrated databases from the analysts' desktops; numerous data sources available on-line (maps and intell reporting) at different security levels; simplified product lines in a limited number of formats; and the ability to receive requests on-line and distribute responses that way. A major investment is required to allow analysts to query, browse and exploit from large, digital image product libraries which use supercomputing and massive data storage technology. Providing this kind of access could greatly increase the amount of time an analyst spends on analysis. Direct interface of imagery with global geospatial information based on a standard coordinate system is required. Automated image examination technology must be pursued. Softcopy exploitation will be the norm; yet softcopy search will require high-speed computing, data storage and management capabilities in the gigaflop range of speed. Tools are needed to accomplish tonal dynamic range manipulation and sharpening, geometric processing for warping or imagery perspective manipulation, and registering images to maps. Data compression, management and display technologies are needed simultaneously. Adaptive image compression schemes will be needed to allow imagery analysts to quickly assimilate information without waiting for the full-resolution image. Greater screen brightness and higher resolution are needed for search. Flat screens with great resolution are needed for tactical situations. Three-dimensional technology will be important (e.g., autostereoscopic, holographic, and lenticular) but screen displays will be needed that do not require special viewing goggles. As imagery analysts search, locate, ID and analyze pertinent imagery, the results will be documented in real-time upon a registered, geographic, information-based, vectored layer. Analytic and presentation aids such as map overlays, terrain displays and 3-D perspectives will be routine. We must capitalize on commonalities among digital imagery and mapping technologies. Superimposition techniques on up-to-date baseline images, maps, and graphics will be able to show changes in force and target dispositions. Such symbolic information overlaid on baseline displays could provide tactical users readily accessible information in a format required for his command and control function. Hardcopy to softcopy conversion must also be a priority due to the vast quantities of historical documents containing text, graphics and pictures that are stored in paper and film form. Conversion

technologies are needed that provide basic indices automatically, preserve formats, and permit full text searches.

One area that remains quite controversial is automated target recognition (ATR) systems. There are many analysts who view ATR systems as direct competition with their jobs. Then, there are others who doubt whether these systems will ever be able to replace the imagery analyst. We have taken a moderate approach to ATR. As stated earlier, we believe that a human will be required in the loop, at least for the next 10-15 years. At that time, it may be possible that technology will have advanced far enough to allow cognitive aspects (i.e., assessing meaning, separating significant from irrelevant data, integrating all available data to form analytical context, making sense of imagery-derived data in the current situation, and judging the significance of the findings) of the exploitation process to be performed by computers. In the interim, we need technology to help analysts be more efficient, not to replace them. Thus, because ATR and artificial intelligence (AI) are a long way from performing these cognitive functions, we recommend increased attention to assisted target recognition (ASTR) systems while continuing low level exploration of ATR systems. R&D must be focused and pursued diligently in these areas for both imaging and spectroradiometric sensing, as ASTR/ATR offer the only major advancement in imagery analysis productivity on the horizon.

ASTR/ATR have the potential to help resolve one of the IMC's biggest problems. In recent years, imagery analysts have been forced to be selective in the imagery they exploit. With the amount of imagery collected increasingly greatly in the near future, this priority-based exploitation will be the norm. The remainder of the imagery will be "binned" into libraries for ready access, if needed at a later date. If no one looks at this imagery at all, nothing will be found. Thus, if assisted "alerting mechanisms" can be developed with low enough false alarm rates to search this excess imagery, then the efficiency of our human analysts is greatly enhanced. There are algorithms of significant value available today that could be used as alert mechanisms. For the future, reliable, totally automated aids to help filter large volumes of data and accurately cue imagery analysts to likely points of intelligence interest will be essential. We should look to architect a system where tasks are efficiently divided between people and machines, parceling out to each the jobs that they do best. Some tasks for computers might be to screen non-literal imagery so an imagery analyst does not have to look at it (as mentioned above). Total automation will depend on what kind of false alarm rate can be tolerated. This will depend on the mission to be supported. Hence, algorithms need to be very specific to the job. We should take the ATR problem and break it up into bins, depending on the problem we are trying to solve. Then we should consolidate the bins and ask ourselves what the value is of doing this automatically. An assessment of that value should be traded against the cost. Computers are persistent but not very cognitive. They can be very

good at search, can find bright spots, can look at certain parts of the spectrum, etc. On the other hand, because computers are much better at certain jobs than are people, in the near-term, we should concentrate on those areas where computers outperform humans and perhaps aim for 50-70 percent automation over the next 10 years. For other processes, we should proceed at a much slower rate and aim for 10-20 percent automation. Early success in automated aids are more likely to occur in filtering large volumes of imagery data to the analysts. High performance image screening and semi-automatic image region cueing also show promise. For the future, ATR needs to move to context-based recognition, not just for single objects for single vehicles, but for units in the field and activity types within fixed facilities. We also need to look at automating exploitation of moving target indicator imagery. If ATR algorithms can be developed that provide a very high level of confidence, then perhaps this processing can be transferred to the collector to allow screening before the data is downlinked. Some enabling technologies that should be investigated include domain mediators (which will help to quickly modify ATR algorithms to different but similar targets) and knowledge engineering tools (automating identification cues, context cues).

- **RECOMMENDATION: Aggressively pursue ASTR/ATR algorithm development, concentrating in the near-term on those areas where computers outperform humans.**

Technology integration for exploitation has not progressed further or more rapidly in the IMC primarily because there exists no single focal point within the imagery community with sufficient influence to foster change. Funding constraints have forced the IMC to focus on procuring only a small part of the full array of needed technologies. No exploitation R&D roadmap exists and different programs seek different technological solutions to similar needs in dissemination, exploitation databases and softcopy. Establishing a funding line specifically for exploitation system development and supporting R&D would assist greatly in addressing exploitation shortfalls. Requiring that such a funding line be tied to each new collection system would ensure adequate "downstream" resources are addressed. Required critical technologies that surfaced during interviews include softcopy exploitation, automated or assisted exploitation, spectral phenomenology, imagery training, multimedia reporting and information infrastructure, surge retrieval visualization and synthesis schools, automated downgrading declassification, and hardcopy-to-softcopy conversion. Exploitation systems must evolve to acquisition timelines of months not years to keep pace with technology changes. For acquisition, we have to accept a 90 or 95 percent solution and not hold out for 100 percent if a commercial capability is available. Recapitalization is another area of concern. What is the optimum recapitalization timeline when what you take off the shelf is obsolete in a year? Other areas that need to be pursued include efficient means of data entry

(like transferring reports to INTELINK) and the capability to precisely align or "fuse" two or more images of the same target but which have been collected from different attitudes, sensors and/or platforms. Newer imagery types (such as multispectral sensing) are harder in terms of their type and the tasks that have to be done for exploitation. A large amount of technology is being pursued piecemeal in this area but there has been no real high priority given to go perform missions in these areas. In the R&D community, we spend an inordinate amount of funds and time constructing databases for testing algorithms. We need a Community, common, controlled test data set and Community standards on metrics so new algorithms can be measured against each other from a common baseline. This would allow for a quick and smooth transition to the analysts' work environment.

The analysts' workstations must be flexible and user friendly. Connectivity via email, at a minimum, with the ability to work on a common white board via personal videoteleconferencing at the individual workstations as a goal, must be implemented among all imagery analysts, both national and military. The IMC should define the standards for imagery exploitation, yet allow decentralized execution. Thus, while the all-source imagery analyst of the future will need more inherent analytic capability than is required today, perhaps the tactical imagery analysts will not if they can correspond real-time with other analysts in a coherent manner. In essence, we must strive toward the "virtual" imagery community. (We would also venture that all analysts, not just imagery analysts, have access to this connectivity, thereby creating a "virtual" IC.) Accordingly, analysts must have user-selectable and filterable theater/national SIGINT-IMINT-HUMINT cross-database query, cueing, and collection request capabilities to facilitate the targeting process and other near-real-time (NRT) requirements. From an IMINT perspective, central digital imagery libraries will be needed and an inventory of available theater imagery should also be accessible on-line. A network of accessible distributed databases integrated with the existing national database should be created. This comprehensive database should have capabilities beyond the current target-oriented systems and allow both imagery analysts and customers to access different levels of information to meet specific needs. In the battlefield of the future, fulfilling those NRT collection, exploitation, and dissemination needs will be critical. Ensuring our timelines are faster than those of our adversaries, especially when those adversaries will themselves have access to military grade imagery, will require implementation of all of these recommendations. These issues must be addressed within the immediate future in order for the imagery workforce to be adequate in the next century. Though some competitive analysis is healthy, the majority of today's isolated and/or redundant imagery production occurs because we are unable to share data, analysis and products between sites. Security measures that guard against unauthorized accesses, both intentional and inadvertent, without stifling system performance, are also required.

- RECOMMENDATION: The IC must move to all-digital exploitation of imagery, with access to cross-INT databases. Move to a "virtual" analytic environment, i.e., one in which analysts are connected electronically. Increase funding to accelerate the procurement of softcopy (digital) workstations for imagery analysts.

The product of the future will be one of merged data from every -INT. They will become less and less textual and more graphical. Geospatially referenced graphical reporting with standardized symbology will become the norm. This will also provide an acceptable method to help protect sources and capabilities. However, the customer must work with these analysts closely before times of crises so that the customer will trust that the symbols are accurate. In this way, perhaps, we can reduce the number of customers who feel they need the raw image, when in fact, all they really need is the imagery-derived data.

This issue, though, may become a moot point, if the "virtual" connectivity discussed above becomes reality. If the new IMC infrastructure is done correctly, users will be able to pull the raw image if he needs it or pull the imagery derived information, all the while retaining email/videoteleconferencing connectivity with analysts within the community. Our perception of CIO's archival plan is that it does not include the raw imagery. This is a mistake. All information should be accessible. If this occurs, the biggest issue will be ensuring that the user who pulls the raw image also takes advantage of the imagery derived data. A common misconception is that the significant intelligence contained in an image is readily apparent to the average observer. While it is true that a consumer, using an identification key, could find on electro-optical imagery an SA-2 site because of its distinctive pattern, the user would not be able to tell if the site were real, dummy, or decoy. Imagery analysis has come a long way from the days of photointerpretation. A comprehensive, analytical, multisource approach to imagery exploitation is now the standard within the National Photographic Interpretation Center (NPIC) and the Defense Intelligence Agency (DIA), though generally not at the force application levels of the military. The IMC must be able to serve both types of customers (force planners and force application end users) and provide support in both types of situations -- where the immediate transmission of raw imagery is enough and where imagery derived information is essential. The "virtual" connectivity mentioned earlier will erase the need to limit the number of raw images required by the user, rendering this contentious issue irrelevant.

Procurement of information processing equipment is, and will continue to be, an incredible challenge for an acquisition system built for the Industrial Age. Trillions of dollars are being spent by industry on information technologies. New products are coming out every six months with new generations of products being produced every 18 months. Our information processing needs cannot survive an acquisition system

that takes five to 10 years to field new systems (6.1, 6.2, 6.3 type funding is unacceptable for information processing systems -- it mandates a long development cycle). We need to modernize our procedures to take advantage of current technology. Our adversaries certainly will. Along these lines, we need to take advantage of commercial advancements and determine whether a commercial product that fulfills 90 percent of our requirements is adequate compared to the cost to customize that product for the extra 10 percent. We need to make maximum use of commercial off-the-shelf (COTS) products which requires someone to inform, encourage, influence and pay vendors to encompass our specialized needs in their technology advancement efforts. Standards are also required so the "guy in the foxhole" can receive imagery data, but government standards need to follow commercial standards if we are to truly benefit from COTS products.

A government-commercial bridge is required, and luckily, one already exists. The National Technology Alliance (NTA) with the National Information Display Laboratory and the National Media Laboratory is that bridge and should be encouraged and expanded. The NTA attempts (and succeeds) in influencing commercial capabilities to encompass government requirements. It provides one set of government requirements that commercial companies can deal with and provides the commercial standards back to the government to influence government decisions. We must practice ways to influence COTS systems before they come to the marketplace so they will be useful to the government. The NTA has been instrumental in saving several government programs while simultaneously influencing commercial standards to better support government requirements. They should be a mandatory participant in any new acquisition of information processing equipment. They should be given the legislative and budgetary freedom to field ACTD-type experiments until commercial companies can pick up the support. The Department of Defense (DoD) might benefit in non-intelligence matters from a similar alliance to help accelerate the fielding of commercial systems.

- **RECOMMENDATION: Expand the purview of the National Technology Alliance (NTA), increasing its resources and flexibility to provide more rapid fielding of new technologies, and to exploit commercially available technology.**

One approach to setting up the imagery processing (data storage, retrieval, etc.) and communications infrastructure, which merits closer scrutiny, is to hire a systems integrator to run this process. Systems integrators (SI) can cut across organizational boundaries (when given that authority) and have the flexibility to recapitalize quickly in areas where technology turns over frequently. These SIs are commercial companies that provide this type of service for a broad array of users.

Their ability to consolidate, delete duplication, quickly upgrade capability and reduce costs provides a model the IMC community should strive to achieve.

Classification

One of the biggest controversies today is the sharing of imagery with our allies in the Balkans. Intelligence data sharing will continue to dominate foreign relations issues for many years. Every day we hear about a new request in ever more divergent areas: environmental, law enforcement, disaster relief, etc. Questions arise: How do we provide the same level of battlefield knowledge to our allies and coalition partners, how do we provide information on disasters, how do we provide data to support U.S. policy decision, all while continuing to protect sources and methods? During the majority of our panels, the customer reiterated that in most cases, he does not require the raw image, only the imagery-derived information. These consumers can be served with graphical overlays which provide the imagery derived information without giving away technical capability. This has worked very well in the support NPIC gives to FEMA (Federal Emergency Management Agency). FEMA provides the LANDSAT or SPOT image and the NPIC analysts overlay those images with a graphical representation using standardized symbology. It is a very efficient process. However, again, in order for the customer to trust the information provided in these graphical overlays, he must train with them.

Of course, in the 21st century, anyone will be able to buy either military grade imagery (one meter) commercially or the actual satellite itself as a turn-key system. Yet, again, we should look to graphical overlays and imagery derived information as the medium we use to share data. We should protect the billions of dollars we invest in these capabilities for as long as we can; once the capability is known, adversaries will undertake countermeasures to defeat/degrade its collection capabilities. In the interim, graphical overlays will have to suffice.

We should also move to protect any future technology breakthroughs. Are we no longer concerned with maintaining a U.S.-only capability and protecting our investments? We need to put back into the psyche of the community that secrecy is a requirement, not an option, especially before we invest dollars in next generation systems. We must move to new collection that is not understood by our adversaries. Along these lines, we should move to develop dissemination systems that can handle multiple levels of classification. Asynchronous Transfer Mode (ATM) technology will allow numerous levels of classification to be passed over the same communications lines. We need to develop the capability to have multiple levels of information accessible from the same workstation.

Dissemination

Dissemination of intelligence information was touted as the biggest failure of the IC during DESERT STORM. Though it remains a challenge today, much has been done at the national level to define interfaces and standards. Communications will be discussed in another *IC21* study, but the bottom line for today is that imagery data can be disseminated to the theater in a timely manner. Below theater is where the problems lie and no national organization is going to be able to fix it. DoD must take the challenge and mandate that each theater's unique mix of national, commercial, and theater imagery needs and systems conform to common dissemination standards and interfaces.

- **FINDING: Imagery dissemination to the military below the Joint Task Force level remains a problem.**

CIO's A3I (Accelerated Architecture Acquisition Initiative) is the right vision: virtual imagery archives accessible at every level. However, here is a program that would benefit tremendously from a Systems Integrator (SI). As stated earlier, these are commercial SIs who have streamlined and reduced overhead for numerous commercial and government ventures, providing "infrastructure" type functions for an overall cost savings. A3I must establish a virtual imagery archive for all digital imagery and imagery products that is easy for users to access. Users will "pull" whatever imagery and products they require. It is in essence, the imagery component of total battle space information to the warrior as envisioned in the C4I concept. Yet, it is really just data storage, archiving and retrieval, and the future we envision will have virtual databases for data from all of the -INTs. Thus, instead of setting up another stovepiped system, we must ensure that A3I will be compatible in the future with a virtual multi-INT data retrieval and archival system. We are not convinced that this is what is occurring and, in fact, A3I has been downgraded because of inadequate funding resources. Also, the military has been very skeptical of A3I because it does not address improvements to the communications network below the CINC level. Though this is not the imagery community's responsibility, an SI might be better equipped to cross organizational lines to implement the infrastructure to support everyone's requirements. In the near term, though, A3I should not be criticized for things out of its purview. An SI might be able to ensure that the communications community is looking at A3I to provide the necessary bandwidth and that, with the advent of global broadcast and direct broadcast service, connectivity via these systems will be easily and quickly incorporated.

Denial and Deception

- **RECOMMENDATION: The IC must continue to examine and to field means by which to overcome "denial and deception" activities.**

Commercial Systems

Commercial systems should be viewed as an adjunct to our national collectors. There are some who believe that the small satellite initiatives and declassification of national imagery will put the commercial companies out of business. However, the commercial imagery companies developed their systems with the aircraft imagery market as their main consumer, not just for the US government (USG). Our prediction is that commercial imagery will be just as important to the USG tomorrow as it is today. It will be a valuable augmenter of the national/tactical systems and the multispectral sensing will provide unique data. One area that should be pursued is whether the commercial systems can provide a "surge" capability that would allow more real time collection/receipt of imagery during a crisis (similar to US Air Force's current ownership of a SPOT collection terminal within the Balkan theater). One sorely needed improvement is a new process for USG users to procure commercial data. The current process takes months, using the Defense Mapping Agency (DMA) as the middleman, and the customer forced to bring his own money. We envision, as part of our imagery organization concept, a central point which would procure commercial imagery as required from a central pot of funding, authorized and appropriated for this purpose. These purchases would be made on behalf of the USG so that anyone within the USG could use the imagery. This imagery would be archived within the main national imagery library where any user could access it. The imagery organization would maintain the index of what imagery had been procured. Of course, the disadvantage to this is that the imagery organization could become the bottleneck for these purchases, pushing the customers to go out and make their own agreements with the commercial companies. This should be allowed as long as the imagery purchased gets incorporated into the national, not just the regional, library, that a consolidated list of imagery purchased is passed to the central repository for indexing, and if a common USG license is issued. This allows flexibility across the board.

- **FINDING: The IC can use commercial imagery more effectively to meet some requirements.**

There are some proposals being considered within the IC that would encourage and allow our allies to buy a medium resolution version of our imagery satellite system. These systems would be exempt from the current "shutter control" mandated by Presidential Decision Directive (PDD-23). The rationale for this proposal stems from

a concern about the US being able to maintain its lead in this technology area because of reduced USG funding. Through these sales, we would have more funding available to invest in future systems while getting increased coverage from these additional systems. This proposal seems to contradict itself; on the one hand, promoting commercial systems is a priority while on the other hand, it advocates building a USG system for foreign military sales (FMS) that would directly compete with those same commercial systems. We are also concerned about giving away our technological advantage in this area. We believe that the shutter control policy is a necessity today. However, we must assume that eventually systems will be proliferated with no such encumbrances and should look to reassess the policy at that time. We also believe that our WFOV small satellite program will not compete with commercial programs or give any more unfair advantage to one program over another. The four licensed programs have all made the decision to go ahead and develop these systems without government funding. Further, the commercial systems would be complementary. By applying adequate collection management, offloading requirements to the commercial systems is a smart move on our part. This would free up our systems to collect other priorities. The biggest difference between our WFOV and the one discussed earlier is that ours would not be made available for government-to-government sales. We would encourage sales of available commercial systems.

- **RECOMMENDATION: The IC must improve its acquisition and use of commercially available imagery. Such imagery can be used in lieu of more costly national assets. As demands to share imagery with non-allies during multilateral operations increases, the use of commercial imagery is especially important to obviate security concerns.**

- **RECOMMENDATION: Set up an account for the easy purchase of commercial imagery, done under the common U.S. government licenses. A central repository and indexing system should be created for easy access by all users.**

MASINT: MEASUREMENT AND SIGNATURES INTELLIGENCE

Executive Summary

As part of the Intelligence Community of the 21st Century study (*IC21*), the Committee reviewed the Measurement and Signatures Intelligence (MASINT) discipline for its relevance in the Intelligence Community's (IC) future. The results of the study reaffirmed some long held beliefs about the relatively unpredictable future -- especially in terms of specific technologies the Community will have to face. One truism that seems to hold is that the sophistication of the technologies employed in the future weapon system (threats that the IC will be tasked against) will be radically improved, and perhaps even more radically different than those we attempt to understand today. The resulting need for a more sophisticated IC collection capability is clear. Clear also, is the need to unambiguously identify these specific weapons or capabilities -- often before they are ever used. Less clear, but undoubtedly true, is the vital role conventional technical intelligence disciplines (IMINT, SIGINT, etc.) will continue to play in the identification and location of the more dynamic targets. However, as the sophistication of these targets increases, or as countries (or transnational players) employ effective denial and deception techniques, we will need to employ new capabilities to ensure we can continue to answer the consumers' questions. One such capability is MASINT. This study concludes that MASINT will take on a more important role than it does today in providing critical information on these future threats. Accordingly, this discipline must be focused and well-managed to ensure the Community can provide the necessary information to its various users.

The study's major findings include:

- MASINT can provide specific weapon system identifications, chemical compositions and material content and a potential adversary's ability to employ these weapons.

- The Central MASINT Office (CMO) has the requisite legal authorities to carry out its responsibilities. However, it is not staffed commensurate with those responsibilities, and a fractured organizational structure limits its overall management abilities.

- MASINT, as a specific and unique discipline, is not well understood by both the IC and user communities. Therefore, the potential of its future contributions may be limited.

- MASINT is both a true, unique collection/analysis discipline and a highly refined analytical technique of the traditional disciplines.

- MASINT straddles strict disciplinary definitions. It may use collection techniques of, but does not fit neatly into any one or all of the more recognized "traditional" disciplines of IMINT, SIGINT, HUMINT, etc.

- MASINT is the least understood of the disciplines and is perceived as a "strategic" capability with limited "tactical" support capabilities. However, MASINT has a potential ability to provide real-time situation awareness and targeting not necessarily available from the more classic disciplines.

- MASINT is a science-intensive discipline that needs people/scientists well versed in the broad range of physical and electrical sciences. Such scientists can not typically be professionally developed with the IC. They must come from academia fresh with scientific knowledge from experimentation and research. Nor can they continue to be "proficient" in their areas of expertise if they remain in government employ for an entire career.

The study's major recommendations include:

- The MASINT technical management function should be contained within the construct of a multi-intelligence disciplined technical collection agency which oversees the coordinated employment of all technical collection systems.

- The IC should create a "U.S. MASINT System" analogous to USSS and USIS.

- The MASINT manager should be a General Officer or SES/SIS and a permanent member of the MIB, NFIB, and other senior DCI and DoD boards/panels. His/Her authorities to manage the MASINT community should be equal to those of the SIGINT and IMINT managers.

- The IC needs to increase emphasis on informing the IC and user communities about MASINT capabilities and products. Additionally, the IC needs to make MASINT a formal course of professional education for all IC school houses.

- MASINT should remain a specific collection and processing discipline. However, MASINT exploitation is becoming more critical as threat technologies improve. Therefore, the IC needs to place increased emphasis on MASINT exploitation within the traditional technical disciplines.

- MASINT planning and system development must focus on not only technical analysis that is necessary for long term signature development, but must also plan, at the outset of any capability development/use, the need to satisfy immediate "tactical" information requirements.

- The IC must be able to tap into any/all U.S. resources, including those not specifically within the IC, that have the ability to input into intelligence data bases. This includes having better access to, and guidance of, national laboratories.

- The IC needs a budgeting mechanism that is equivalent of "ready cash." This would provide the ability to readily fund fleeting or promising technologies, R&D efforts (without penalty for those technologies/or scientific breakthroughs that do not bear fruit), or unplanned operational opportunities. This authority needs to be analogous to a venture capitalist.

- The IC needs to examine the feasibility of pursuing trial personnel management programs that provide incentives to recruit and maintain the necessary scientific experts.

MASINT: MEASUREMENT AND SIGNATURES INTELLIGENCE

Study Purpose

One can argue that the requirements levied on the Intelligence Community (IC) in the twenty-first century will not be radically different than those levied on it today. The basic information needs of "who, what, where, when and why" will likely not change. However, most can easily agree that the sophistication of the technologies employed in the future weapon systems (threats) that the IC will be tasked against will be radically improved, and perhaps even more radically different than those we attempt to understand today. Increasingly, even unsophisticated countries are gaining access to relatively inexpensive, but high technology weapons. Weapons that can be "launched and forgotten," weapons of mass destruction -- including nuclear, chemical and biological, or weapons that are difficult to detect or are stealthy. The resulting need for a more sophisticated IC collection capability is clear. Clear also, is the need to unambiguously identify these specific weapons or capabilities -- often before they are ever used. The IC's ability to specifically locate, identify, characterize, and determine the intentions of such weapons or threats is, and will become even more, critical. Conventional technical intelligence disciplines -- Imagery Intelligence (IMINT), Signals Intelligence (SIGINT), etc. -- have played, and will continue to play, a vital role in the identification and location of such targets. However, as the sohpistication of these targets increases, or as countries (or transnational players) employ effective denial and deception techniques, we will need to employ new capabilities to ensure we can continue to answer the consumers' questions. One such capability is Measurement and Signature Intelligence, or MASINT. MASINT is a very scientific and technically-based discipline that can provide unique contributions to the IC in terms of specific weapon identifications, chemical compositions, material content, etc. Such unique identifications will be a major factor in answering the future questions of "who, what where, when and why." In fact, some believe MASINT will be the most important "technical INT of the future."

Despite the clear criticality, both present and future, of the MASINT discipline, it is the least well known of the technical collection/analysis disciplines. Many have questioned the nature of the discipline: is it a true collection discipline or is it a unique product based on specialized analysis? Few who have had the opportunity to review MASINT products, however, can dispute their utility, or the current and growing need for these products. The purpose of this study, therefore, was to determine several specific issues relative to MASINT. First, was to identify the viability and need for MASINT-unique collection and processing in the 21st Century. Second, was to determine the IC's strengths and weaknesses in providing such necessary MASINT support. This was to include making any recommendations for necessary changes to systems, architectures, management, technologies requiring emphasis, etc. to ensure

the discipline's viability. Finally, we wanted to address the budget implications of attempting to achieve these goals.

Study Approach

It should be first noted that this is not a scientific study, but rather an assessment based on community expert inputs. To get substantive input for the study, the staff team sponsored several round-table panel discussions, numerous individual interviews, and formal presentations with MASINT Committee members, the Services, the Defense Intelligence Agency (DIA), Arms Control professionals and former community officials. The effort was designed to "think out of the Future Years' Development Program (FYDP) box." That is, there was no attempt to indict the past, present, or programmed organization and efforts, but rather to look "beyond" into the future. The team developed an outline and series of questions to prompt inputs/discussion from each of the invited participants. The approach viewed MASINT as a distinct collection discipline even though the discipline is not well bounded by specific (and unique) collection and exploitation definitions. Our effort focused on identifying the current capabilities and systems trying to determine their individual contributions and where each should/could be best employed in the future. However, the sciences and rapidly evolving technologies involved eventually focused us more toward a review of MASINT management, including the abilities to coordinate and program for new sensors/technologies, to task sensors, and to use and disseminate MASINT information. Recommendations from participants were noted and, to the extent possible, identified in this report.

Secondly, it also needs to be noted that the recommendations offered below were originally focused on a MASINT management and operational structure that was generally maintained within the current IC organization. And, although these recommendations were made before the completion of the *Intelligence Community Management* staff study, they work well within the construct of that study's more consolidated community organization. Specifically within the context of that study, all references to the "Central MASINT Office (CMO)" are assumed to be describing a division (or office) within the Technical Collection Agency (TCA) under the Deputy Director of Central Intelligence for Community Management (DDCI/CM). If the TCA construct is not adopted, the CMO references describe the Community's MASINT management organization assumed to be within the DIA.

Finally, in addition to the panel discussions and interviews, the team reviewed and used the following supporting documents during the study:

A. MASINT Handbook for the Warfighter, prepared by the INCA Project Office, November 1994

B. CMO Biological and Chemical Warfare Intelligence Collection Strategy Briefing, R. Paul Schaudies, Ph.D., November 1994

C. CMO Investment Process Briefing, Mr. Dale Helmer, August 94

D. CMO MASINT Master Plan, January 1994

E. MASINT 2010 Study, October 1995

F. Director of Central Intelligence Directive 2/11-1, December 1992

G. DoD Instruction 5105.58, February 1993

H. DoD Instruction 5105.21, May 1977

Background

A general understanding of the genesis of MASINT and its official definition is appropriate prior to a study regarding the future of the discipline.

Recognizing the need to ensure proper exploitation of complex, technically-derived data, the IC classified MASINT as a formal intelligence discipline in 1986. At that time, the IC Staff MASINT Committee was formed to oversee all MASINT activities. To further consolidate MASINT management, the Central MASINT office (CMO) was established in 1993 by the Director, DIA, with specific responsibilities detailed by the Director of Central Intelligence (DCI) and Department of Defense (DoD) Directives. The CMO is a joint IC and DoD activity within DIA, that directs and implements national and DoD policies and procedures on MASINT matters. With that quick background, it is useful to identify the IC's current official definition of MASINT:

> Measurement and Signature Intelligence (MASINT) is technically derived intelligence (excluding traditional imagery and signal intelligence) which when collected, processed, and analyzed, results in intelligence that detects, tracks, identifies, or describes the signatures (distinctive characteristics) of fixed or dynamic target sources. MASINT includes the advanced processing and exploitation of data derived from IMINT and SIGINT collection sources. MASINT sensors include, but are not limited to, radar, optical, infrared, acoustic, nuclear, radiation detection, spetroradiometric, and seismic systems as well as gas, liquid, and solid material sampling systems.

Despite this definition, many in the IC (and policy community) are confused as to what MASINT really is. Although MASINT can be described as the highly technical exploitation of traditional disciplines, the MASINT collection techniques cover areas not addressed by other disciplines. In many respects, there is a clear distinction between MASINT and the other disciplines. MASINT can be considered analogous to the individual who relies on all senses to gain information about his or her environment. Where SIGINT is akin to sound, and IMINT to sight, MASINT is akin to touch, taste and smell. The areas where MASINT expands on the traditional disciplines (IMINT and SIGINT) can be thought of as providing aids to improve upon or add dimensions and capabilities to the sight and sound senses that would not otherwise be possible. Is MASINT a true collection discipline, or is it actually specialized processing of other collection disciplines? Is it a separate field of specialization, or more appropriately classified as additional processing and analysis of existing data? These questions were a fundamental basis for the study that went into this report. Specifically, we tried to determine how to correct this "identity crisis," while ensuring the community will be served by the truly unique product MASINT can provide.

General Conclusions

Based on the various inputs, the group identified six general conclusions that appear to sum up the general issues relative to MASINT. Each of the general conclusions are later broken down into specific conclusions and recommendations.

A. MASINT is difficult to bound by strict definitions. In fact, MASINT collections can, in part, legitimately be labeled as SIGINT, Infrared Intelligence (IRINT), IMINT, HUMINT, etc. However, MASINT does not fit neatly into any one or all of these recognized "traditional" intelligence disciplines. MASINT is both a true, unique, collection/analysis discipline and highly refined analytical techniques of those traditional disciplines. Despite these gray lines of demarcation, MASINT may be the "intelligence discipline of the future" -- that is, MASINT is a discipline that is becoming more important in identifying and characterizing new and emerging threats, particularly as weapon system technologies become more complex and capable. Without a robust and focused capability, MASINT's support to future needs, such as "brilliant" weapons and national information requirements (e.g., weapons proliferation, arms control, force modernization, strategic programs, scientific and technical needs, environmental and humanitarian concerns, and counter-narcotics/terrorism), may be inadequate.

B. MASINT is perceived as a "strategic" discipline with limited "tactical" support capabilities. But, by application of real-time analysis and dissemination, MASINT has a potential ability to provide real-time situation awareness and targeting not necessarily available to the more classic disciplines. Because

of these perceptions, MASINT does not get the attention of the tactical consumers, and has less constituency support than the more traditional intelligence disciplines. Lacking proper constituency, MASINT sensors and analysis will likely not be properly supported or maintained. Results will include a lack of targeting templates for smart weapons.

C. MASINT, as a specific and unique discipline, is not well understood by the IC as a whole. Therefore, although it provides significant intelligence products, its contributions, or the potential of its contributions may have been and will likely be limited. The full extent if its future application to national and operational intelligence will not be realized.

D. Funding levels for the current MASINT systems, and those projected into the future are not reflective of the importance of this discipline to the Nation's general intelligence/ dominant knowledge efforts. This is primarily because users do not have direct tasking over, and therefore understanding of, MASINT sensors.

E. The roadmap for specific MASINT technologies appears to be fairly well thought out and necessary for the 21st century. However, there may be insufficient funding flexibility for reacting to, or pursuing new, emerging, or fleeting technologies. Additionally, there is a need to ensure a balance between the requirements and technologies that support military battlefield requirements, and the often more exacting requirements and technologies that are needed for IC national monitoring and detection of weapon or agent developments.

F. Although the CMO has the necessary legal authorities, it is not properly staffed commensurate with its responsibilities. Additionally, a fractured organizational structure provides little to no focused MASINT management, budgeting oversight, tasking control, or coordination of effort. This may potentially cause inefficient expenditures of resources and duplicative developments.

Specific Conclusions/Findings

A. "MASINT is difficult to bound by strict definitions. In fact, MASINT collections can, in part, legitimately be labeled as SIGINT, IRINT, IMINT, HUMINT, etc. However, MASINT does not fit neatly into any one or all of these recognized "traditional" intelligence disciplines. MASINT is both a true, unique, collection/analysis discipline and highly refined analytical techniques of those traditional disciplines. Despite these gray lines of demarcation, MASINT may be the "intelligence discipline of the future" -- that is, MASINT is a discipline that is becoming more important in identifying and characterizing new and emerging

threats, particularly as weapon system technologies become more complex and capable. Without a robust and focused capability, MASINT's support to future needs, such as "brilliant" weapons and national information requirements (e.g., weapons proliferation, arms control, force modernization, strategic programs, scientific and technical needs, environmental and humanitarian concerns, and counter-narcotics/terrorism), may be inadequate."

1) One discussion point focused on whether to maintain MASINT as a separate discipline or to break it up into the separate disciplines (i.e. Radiation Intelligence (RADINT), SIGINT, IMINT, etc.). This discussion focused on whether or not to make MASINT professionals organic to the traditional intelligence disciplines or keep them separated within the distinct discipline. Some believe that doing away with the unique professional MASINT discipline that cuts across the other disciplines' collection spectra would be counterproductive. They believe better coordinated MASINT products are possible when viewed across the various collection disciplines. Their argument for maintaining a separate MASINT discipline states that such "cross cutting" is providing positive results in terms of all-source analysis. Upon close inspection this is apparently true. However, there is a counter-argument that includes the issue of refined "technical" exploitation of the "traditional intelligence disciplines" (explained below). This counter-argument focuses on the need to "proliferate" the MASINT exploitation potential to other disciplines. Regardless of the whether MASINT remains a distinct discipline or not, there is a need to redouble efforts to get people of different "intelligence stovepipe" expertises together doing true all-source (including non-intelligence sourced information) analysis.

2) As touched on above, a counter-argument is that MASINT, as a term and as a separate discipline, may not be what is needed for the 21st century. A specific case can be made that MASINT is simply more refined, more scientific and more technically challenging analysis of existing collection[1] (although much MASINT collection is done outside the realms of other existing collection disciplines). However, one respondent (favoring maintaining a separate discipline) stated, "Frankly, the MASINT odds and ends (e.g., phase history data) that could belong to other intelligence disciplines would probably not exist today if the MASINT phenomenologists had not pursued them." This may be true, but the question still exists which asks "Is MASINT a separate collection discipline or is it IMINT, SIGINT, HUMINT, IRINT, or other disciplines in their various forms?" Further, if the answer to the latter is "yes," then one has to ask whether MASINT is then the more detailed exploitation of those available collections. This argument

[1] MASINT panel #3 discussions; individual responses to MASINT questionnaire

becomes less clear, and the apparent answer to the first question becomes "no" when one studies the clearly MASINT-unique collection systems, entities and missions such as seismometry, nuclear and soil sampling.

The argument for subsuming the MASINT discipline assumes that the MASINT product is not-so-simply the result of more in-depth analysis of the "traditional" intelligence disciplines. For example, although COBRA BALL is clearly a MASINT platform, its collection media are multidisciplined, and include IMINT (visible and non-visible spectra). The product distinction is more in the resulting analysis and use of the data collected via these disciplines' means. The product then, rather than being used for the traditional intelligence support functions of counting tanks, locating battalions, and targeting ATACMS missiles, is used for scientific/technical refinement to do signature and capability analysis. The basic sciences (between MASINT and the other disciplines) are not altered or different, but the state of refinement is. Another example is effluent analysis based on hyper-spectral collection. The collection is, arguably, IMINT in its various (non-imaging) spectra, but the product is fundamentally different analysis of the effluent content -- not just the detection (or imaging) of presence. This argument would question whether MASINT tasking, analysis and expertise need to be better developed within the existing "traditional" intelligence disciplines.

3) Another argument for maintaining MASINT as a distinct discipline is captured in the following. Specifically, MASINT seeks to collect metric data and signatures. Metric data are derived from the direct measurement of the kinematics performance of targets of interest. Metric data provide information on the dynamic capabilities of targets and/or the tactics for their use. Signature data typically are -- or are derived from -- "high-fidelity measurements of targets of interest, in the context of their application, use or production, to allow the current or future unique identification of such targets." SIGINT, as its name implies, is based on the desire to intercept or collect signals -- the transmission of information from one place to another. Intercepted signals could contain information on a wide variety of topics that overlap information collected by IMINT or MASINT means; but the collection is still SIGINT. IMINT endeavors to provide pictorial representations of targets and areas of interest -- not the spectral analysis of material content. All three technical collection disciplines employ electro-optical (EO) - and radio frequency (RF) -- based systems to provide unique MASINT, SIGINT, and IMINT collection capabilities. However, and additionally, MASINT also makes use of a wide range of other measurement techniques such as seismic, acoustics, magnetic, and nuclear, to provide capabilities against targets that cannot be prosecuted using EO- or RF-based systems. In summary, intelligence disciplines are differentiated on the basis of the type

of information being collected and extracted through processing and exploitation -- not on the physical basis of the collection system employed or the intelligence problem being addressed. This argument attempts to justify the need to maintain MASINT as a separate discipline. This is a good argument and position, but perhaps one that is bound by the "current think" box.

Findings/Recommendations (There are several, possibly conflicting recommendations which need to be discussed/debated)

4) **There are several possibilities for ensuring the MASINT capability into the future. The first would be to delete the term MASINT from the IC's vernacular. This option would place MASINT collection and exploitation functions within the auspices of the other collection disciplines. This would require replacing the term with a deeper understanding, and, moreover, appreciation for the fact that more exploitable information is available (much within the current discipline collections) than what is being used today by the "traditional exploiters" (those unique collections traditionally identified as "MASINT" not withstanding).** This understanding will **require the employment of scientific and technical people (the current "MASINTers") within the traditional intelligence organizations (the services, NSA, CIO, etc.), and force more "traditional collection" in the areas of sampling, etc.** This is to say that specific, technically-astute (MASINT) individuals need to do this; it most likely cannot be done by people who are experts in the known collection and exploitation functions of the traditional disciplines. However, **there is a danger in deleting the term**, and putting "MASINTers" in with the more traditional disciplines. These people may eventually "get lost" in the traditional disciplines' focused charters and the technical and scientific exploitation will be lost. This was the reason the MASINT discipline was created in the first place. Additionally, deleting the term would force other approaches at non-traditional collection such as seismic, thermal, etc.

5) The second possibility is to maintain the status quo and retain MASINT as a specific discipline. This does not improve the problems we see today with the identity of MASINT.

6) **The third is a "hybrid" of the two options above. That is, MASINT should remain a specific collection and processing discipline with its core of professionals and management staff. However, the more traditional technical disciplines of IMINT and SIGINT should specifically address, in their charters, the recognition of the MASINT ability to glean additional data from their collections (this would be facilitated by the TCA construct).** This would require the deeper understanding, and associated dedicated people identified in the paragraph above. **Additionally, MASINT should be treated just as are**

the other technical disciplines in that the IC should Create a "U.S. MASINT System" with associated functional manager (the CMO). This would still be logical within the structure of a TCA. Finally, based on the outcome of the *Intelligence Community Management* staff study, **the Committee recommends the MASINT functional manager (FM) (the CMO) be subordinated to the TCA for logical management.**

7) The basic sciences (between MASINT and the other disciplines) are not altered or different. It is the state of refinement (of the technical or scientific analysis), often the collection source (e.g. the case of soil or effluent sampling) and nature of data being pursued that are the differences.

8) MASINT tasking, analysis, and expertises need to be better developed within the existing "traditional" intelligence disciplines. Specifically, the more traditional disciplines need to have a better understanding and appreciation for the facts that additional exploitable (MASINT) information may exist within their current collections. This requires the deeper understanding recommended above, but also requires a specific oversight organization (the current CMO) to ensure this refined analysis and IC direction.

B. "MASINT is perceived as a "strategic" discipline with limited "tactical" support capabilities. But, *by application of real-time analysis and dissemination, MASINT has a potential ability to provide real-time situation awareness and targeting not necessarily available to the more classic disciplines*. Because of these perceptions, MASINT does not get the attention of the tactical consumers, and has less constituency support than the more traditional intelligence disciplines. Lacking proper constituency, MASINT sensors and analysis will likely not be properly supported or maintained. Results will include a lack of targeting templates for smart weapons."

1) As stated previously, MASINT is, in some cases, the more scientific analysis product of the more traditional collection disciplines. Because of the highly technical means utilized, most MASINT systems' focus has been on the longer-term (i.e., not "real-time") analysis of data to determine characteristics, signatures, target templates, etc. With the advent of modern processing techniques and capabilities, MASINT systems have an increased potential for doing their analysis in near real- or real-time. Such potential MASINT contributions to the requirements of tactical customers is poorly known -- and in some cases not being pursued.

One example of MASINT contributions to real-time identification is the application of MASINT signature data for non-cooperative target identification (NCTI). Today, U.S. systems have a capability to identify hostile fighter aircraft based on MASINT techniques. However, it is poorly known that this

analysis was done by MASINT resources. Because of the "unknown sources" for such capabilities, constituency concerns can arise during budget formulations when the participants have a poor or no understanding of MASINT (or other intelligence) applications. Decisions whether to fund intelligence sensors or additional technologies -- such as NCTI -- on offensive weapons can be skewed, based on these lack of understandings. For example, funding debates that are "pro-intelligence" (versus "operational") may be short-lived and the original contributing capability (e.g., a MASINT sensor) is the loser. It must be continuously recognized there is a basic difference between the general sensor approach for "warfighting" and the specific, often more sophisticated, sensors necessary for intelligence collection and knowledge-making. Intelligence sensors must have the ability to measure and define fully the target threat or signature needed. Therefore, these must have full spectral coverage, dynamic range, etc. The resulting "battlefield sensors" employed by users often can be more simply designed to recognize the presence of a threat based on the signatures provided by intelligence. The importance of this thought cannot be underestimated.

2) Despite its "strategic" intelligence past, MASINT has a critical and growing role in future real-time "warfighter" support. Specifically, MASINT "sensors" have unique capabilities to detect missile launch, detect and track aircraft, ships, and vehicles, do NCTI and battle damage assessment, and detect and track fallout from nuclear detonations. Often, these contributions are the first indicators of hostile activities. The shootdown, for example, of the two EXOCET-equipped Mirage F-1s during the Gulf War was attributed to a MASINT collection and analysis.

3) MASINT, or the "MASINT applications" of SIGINT and IMINT (etc.), will become more important in providing the future inputs for smart weapons target templating. That is, MASINT is critical for providing future weapons with the signatures (fingerprint) of the targets they are seeking (IR signatures for example).

4) MASINT sensors are often the same systems as "warfighting systems." The difference is often only the level of sophistication of the data analysis. A specific example is the use of data available from operational radars incidental to the targeting functions for which these radars were built. AEGIS radar returns contain data that can provide significant metric data for assessing weapons system performances.

Findings/Recommendations

5) MASINT planning must focus on not only the technical analysis that is necessary for long term signature development, but must also plan, at the outset of any capability development/use, the need to satisfy immediate information requirements for the tactical consumer. This means that MASINT planners must coordinate with the information users at the inception of a program to determine, at a minimum, the needs to be satisfied, the format for display of the information required, and addressing human factors issues such as amount of data, timeliness of data, etc.

6) MASINT systems should be provided with the capability to communicate with/broadcast directly to customers just as do the "traditional intelligence disciplines." This should include an assessment of the utility of broadcast systems such as the Tactical Information Broadcast Service (TIBS) and other data links. The specific implementation of this recommendation should be developed by the DDCI/CM's Infrastructure Support Organization (see *Intelligence Community Management* staff study).

7) **MASINT culture must be changed to think of analysis in terms of seconds and hours AS WELL AS its current months and years.** This requires school house concentration on MASINT curriculum, and an everyday appreciation with the traditional disciplines. This also demands that users be involved and informed relative to MASINT capabilities.

8) *Specifically identified MASINT systems are not the only sources of MASINT data.* Targeting radars, for example, can provide ancillary data useful to the national collection/analysis efforts. **CMO must have 1) insight not only to specifically identified MASINT systems, but also to those offensive weapons systems (radars for example) capabilities that can contribute to technical and scientific (MASINT) information data bases; 2) when necessary, have the wherewithal to request/suggest/ask for tasking authority for these systems.** Additionally, **CMO should have a funding ability to provide "seed" money to determine or improve MASINT exploitation of existing weapon system data.** This will require a "rethink" that "intelligence and its sensors" are not something strictly unique, but rather *"intelligence and its sensors" are the totality of information available to the U.S. government.* The national defense psyche must not continue in the "we" (operations)/"they" (intelligence) construct.

9) *CMO needs a better understanding of user needs, not just stated requirements.* This demands that the intelligence and user communities (particularly the MASINT community in this case) coordinate and talk more. The security barriers to effective communication must be broken down. (They are to some extent, but this must be expanded.)

C. "MASINT, as a specific and unique discipline, is not well understood by the IC as a whole. Therefore, although it provides significant intelligence products, its contributions, or the potential of its contributions may have been/will be limited. Its future application to national and operational intelligence will not be maximized."

1) Despite the formal definition, MASINT remains an intelligence discipline enigma. It is more diverse and unique than the more focused IMINT and SIGINT disciplines. It is characterized by some as having some similar sources and methods (of the more classic disciplines), but much more complex, particularly with respect to analysis than those others. MASINT has many of the collection characteristics of the other technical disciplines, however, it is the unique exploitation and unique techniques that distinguish MASINT results. One respondent stated that MASINT products are the intelligence bits remaining after the expected results of collection are removed. Another stated that MASINT provides alternatives that supplement "conventional" collection to provide "the rest of the story."

Some would say it is the unique data retrieved from additional processing -- the technical and scientific data -- that can set the MASINT discipline apart from the host intelligence discipline." However, MASINT collection and processing are not limited to the phenomena of the electro-magnetic (RF) spectrum. Significant MASINT information is derived from seismic sensors, acoustic sensors, nuclear radiation sensors and material/effluent sampling. This identity crisis becomes troubling when there is a choice to be made, particularly in funding issues. Some state there is no identify crisis for MASINT, that there is, instead, a need for IC and customer education. This education need does, indeed, reflect the identity crisis discussed above.

2) The CMO and INCA have developed a guide called the MASINT Handbook for the Warfighter. This document has been printed and distributed to "demystify the world of MASINT." This handbook is a critical start toward educating the community and users in the art of MASINT. It needs to be "standard issue" throughout the IC.

3) As stated briefly above, the MASINT "identity crisis" is also apparent when there are budget cuts to be made. As one respondent noted, MASINT

is the "soft underbelly," which is "easily cut" during budget cut drills. Whenever there are cuts to be made within the IC (i.e., GDIP), MASINT (particularly Research and Development (R&D) funds) are some of the first to be targeted.

4) There was much discussion on the need to improve formal initial and continuing education within the IC[2] for MASINT professionals. Formal scientific/technical, mathematical and engineering skills are critical backgrounds for MASINT professionals who do the detailed exploitation of MASINT data. Training for these backgrounds is not typically done within the IC; it is more a function of academia. To get the necessary professionals, the IC must be able to recruit "MASINTers" from the professional (research/laboratory) and academic worlds. Continuing education needs to be both "in-house" and fostered within the private/professional sectors.

5) MASINT has no formal/viable method (i.e., metrics) for evaluating MASINT contributions to the IC or user communities. That is, there is no formal method for determining whether MASINT analysis and products are satisfying the needs of the customers. This was specifically characterized by the unbalanced MASINT results of the recent Community-wide Capabilities Analysis. There is a need to develop a metric or set of metrics to determine the impact of MASINT products toward stated knowledge goals.

Findings/Recommendations

6) The services and agencies need to do a better job of educating the user and, moreover, the IC, on the capabilities, applications, and specifics of MASINT. **MASINT (familiarity) should become a formal course of professional education for all IC school houses. Existing courses, that include MASINT content, should be increased in scope and duration. Specific tailored courses should provide a curricula that cuts across the spectrum of general user overviews to in-depth analytic instruction.**

7) **The MASINT User's Handbook should be required reading within the IC. Additionally, recommend the MASINT User's Handbook be developed in both all-source and unclassified versions.**

---

[2] MASINT Panel #1, #2, and #3 discussions and individual interviews.

8) Continuing IC education should emphasize the unique collection and products of MASINT, and more specifically, the MASINT (technical and scientific) applications of individual "traditional" disciplines. That is, IC professionals within the IMINT and SIGINT fields should be made more aware of the contributions MASINT analysis can make to existing IMINT/SIGINT collections. They need to be made aware that additional information may be gleaned from existing collections once the "expected information has been stripped away."

9) Education, particularly continuing education, of the IC cannot be overstated. The CMO has developed an updated video tape that highlights MASINT contributions. This video tape is an information sharing source that should be exploited to the extent possible. The IC should share this tape with all IC components and users. This tape, or like, should be shown at the school houses and at operational intelligence organizations to publicize the contributions of MASINT collection and analysis.

10) CMO should pursue an adjunct training capability, with trained instructors, like that of NSA to ensure MASINT training is conducted and maintained. This training facility should be reviewed for both "in-house" and exportable training efforts. CMO should be a "clearing house" for developing such training materials, including "for credit" courses. Funding for this should be a CMO responsibility, with the necessary resources programmed and provided.

11) There is a need to develop and maintain evaluation criteria (metrics) to gauge MASINT customer needs satisfaction. The National Intelligence Evaluation Council (NIEC -- within the recommendations of the *Intelligence Community Management* staff study, the NIEC is an organization subordinate to the DCI and responsible for evaluating the Communities satisfaction of requirements) should develop both evaluation criteria and a program for measuring MASINT product effectiveness. This is necessary to determine future needs and the ability to satisfy those needs.

12) CMO needs to provide more community emphasis on educating the user (warfighter and policy makers) on the utility of MASINT products and services. Specifically, the service War Colleges, for example, need to increase the blocks that teach intelligence to all future leaders of the Armed Forces. MASINT must be a formal block of instruction in such courses. Again, without a basic understanding of what the product can provide, the customer typically has no appreciation of the need for MASINT and the associated expenditures of funds. Without such an appreciation, the discipline may be under-utilized.

D. "Funding levels for the current MASINT systems, and those projected into the future are not reflective of the importance of this discipline to the Nation's general intelligence/ dominant knowledge efforts[3]. This is primarily because users do not have direct tasking over, and therefore understanding of, MASINT sensors."

1) R&D is the lifeblood of MASINT. However, MASINT R&D funding is one of the most vulnerable to being cut within the GDIP program. Low obligation rates and lack appreciation for R&D's future contributions make this an easy target which is often hit during cut drills/actions.

2) Funding levels are considered by the group as relatively reflective of the current need. CMO's long range technology plan, with associated expected costs, is good, but does not allow for the unknowns of scientific breakthroughs or unforeseen technology needs. The disparate organizational "ownership" of the funding does not allow for coordinated/effective expenditure of the available funds.

3) MASINT requires, in many cases, single (to several) technical collections systems, this forces paying "prototype costs." This is a cost intensive effort that needs to be acknowledged up front. Pure scientific research is the bread and butter that must be funded at a continuing level. There is a need for level-effort-funding like that of the laboratories, that is not cut for convenience. Additionally, the MASINT community must do better in terms of coordinating efforts with the national laboratories.

Findings/Recommendations

4) MASINT resources and funding needs must be better managed and coordinated between the services, agencies, and laboratories. **CMO must be provided (or assume) better insight into each of the MASINT programs.** This should include providing recommendations into MASINT system POM builds. **However, the recommended DDCI/CM's Community Management Staff (CMS) should construct the coordinated budget.**

---

[3] Panel respondents, MASINT panel # 1, 2 and 3 discussions.

5) *MASINT R&D efforts must be better coordinated to ensure proper level of effort and minimize redundancy.* **CMO should be given authority to have specific insight into the national laboratory and ARPA developmental and research efforts, and should have the ability to focus or request research and experimentation. This should include a level-of-effort funding program, controlled by CMO to do required research or to assist a promising technology. CMO should be given the authority to directly obligate funding. This recommendation is greatly facilitated by the TCA and Technology Development Officer (TDO) organizations under the DDCI/CM.**

6) **CMO should be given additional budget authority to control a "to be determined" amount of funding to be applied to existing intelligence and operational systems to determine/improve their MASINT data collection potentials.**

7) **CMO must be directed to specifically prioritize MASINT systems (agency and service included) for funding purposes.** Such authority must recognize that CMO does not have jurisdiction over "multi-role" platforms (those that can accomplish "MASINT collection" as incidental to their primary tasks).

E. "The roadmap for specific MASINT technologies appears to be fairly well thought out and necessary for the 21st century. However, there may be insufficient funding flexibility for reacting to, or pursuing new, emerging, or fleeting technologies. Additionally, there is a need to ensure a balance between the requirements and technologies that support military battlefield requirements, and the often more exacting requirements and technologies that are needed for IC national monitoring and detection of weapon or agent developments."

1) CMO has developed a technology roadmap, complete with projected cost data. This effort appears to be logical and complete with necessary analysis. However, the roadmap does not provide well for the unknown. That is, there are always the possibilities and probabilities for future new and emerging technologies or requirements that cannot be specifically planned for. There is a need to be able to capitalize on these unforeseen breakthroughs. This is the need to "plan for the unknown."

2) Relative to "intelligence versus operations," there appears to be a specific coordination problem with MASINT versus counter-proliferation efforts against weapons of mass destruction and, more specifically, chemical and biological weapon (CW/BW) proliferation. Current efforts are not well coordinated and resources are scattered throughout the U.S. government. For example, the Under Secretary of Defense for Nuclear Policy has significant resources available for the defense of or counter proliferation efforts against CW/BW weapons. CMO has little to no insight or direction

into the "intelligence-related" activities. Additionally, without better insight, the CMO's MASINT roadmap will pursue duplicative efforts.

3) There is a critical difference between battlefield support to military operations (SMO) MASINT requirements, and those requirements for detecting, for example, the early stages of a weapon or chemical agent development. Much MASINT and, indeed, all other disciplines' emphasis is placed on SMO. However, the criticality of developing and maintaining extremely sensitive sensors for ensuring the Nation's ability to monitor, detect, characterize and classify developmental weapons/efforts, such as biological, chemical and nuclear, cannot be overemphasized. There are specific requirement differences, for example, in designing battlefield chemical detectors that "simply" identify the presence of agents, and the more sophisticated sensors designed to provide the in-depth collection and analysis for knowledge of the characteristics of these agents. This requires a balance of emphasis to ensure that "non-SMO" intelligence requirements are met.

Findings/Recommendations

4) **CMO should be provided with a level-of-effort budgeting capability. That is, CMO should request, and Congress should provide (via legislation) for, a budgeting mechanism that is that equivalent of "ready cash" or venture capital.** This account should be used to pursue new or unexpected technologies, react to unforeseen requirements, etc. Such a funding mechanism is becoming increasingly critical as technology turnover times decrease. **CMO should have the specific authorized ability to direct funding against, or to pursue such promising technologies or R&D efforts (without penalty for those technologies/or scientific breakthroughs that do not bear fruit).** This authority needs to be analogous to a capital venturer.

5) As with the "tactical" systems, **CMO should have direct insight and influence over Weapons of Mass Destruction (WMD) efforts -- most specifically on the intelligence related issues.** There is a great potential to more closely coordinate efforts and provide a more cohesive national defense. **A CMO specialist should be assigned to organizations working WMD programs to improve the cross-flow of information on current and planned capabilities/operations. Barring this, CMO should be a formal invitee to any/all discussions that focus on this area.**

6) *Bistatics (RF) need more attention.* Bistatic RF solutions are poorly understood/appreciated within the traditional disciplines. This area needs more study and resources put against it. Bistatic solutions provide a unique opportunity to provide real-time NCTI and for reducing friendly fire losses.

7) **CMO needs a continuous, broad review of all government, and to the extent possible, commercial developments to determine the most logical and cost effective MASINT potentials.**

8) **The community must maintain proper emphasis on both SMO and "non-SMO" aspects of collection and analysis.** *The often more sophisticated and difficult processes of intelligence collection and processing for detailed knowledge of weapons systems, material content, molecular compositions, etc., require markedly different sensors and techniques which the IC must pursue.* **Such collection and analysis capabilities cannot be overemphasized.** *It is these techniques that provide the knowledge base for developing the battlefield SMO systems.*

9) *Promising technologies which need current and future emphasis include:*

a. *Target signature data bases.* These data bases will be the future "targeting systems" for smart/brilliant weapons. These data bases will also provide the potential "countermeasures knowledge" for development of future defensive systems. These data bases need improvement and application (and perhaps maintenance) at the "shooter" level.

b. *Continual, coordinated sensor development (as science and technology advances)* in space, air ,sea, and ground. There is a need to ensure all developments -- whether they are "intelligence" or "operations," and despite the medium in which they are intended to be employed, are coordinated to determine their information production potentials.

c. *Refined signal processing that is applicable to all intelligence disciplines.* Technology advances that are worked in one area of the IC must be shared throughout the community. Far too often an agency or organization creates a collection or processing technique or capability that has much potential for other in the IC. There needs to be a vehicle whereby such developments can be shared.

d. *Multi-sensor/data integration between diverse intelligence disciplines and within disciplines*. Again, there is much to be gained from synergistic collection and analysis. This must become the "business norm" throughout the IC.

e. *Wide area surveillance technologies employing target signature identification methods.* Such technologies hold the promise of improving automated recognition algorithms for improving analyst productivity.

f. *MASINT system direct integration with other intelligence collection and operational (warfighting) sensors.* Again, the concepts of multi-discipline intelligence analysis and the immediate (tactical) use of such available information will be crucial to future needs satisfaction.

g. *Multi-spectral signatures.* Current and future generations of smart weapons; Theater Ballistic Missile Defense (TBMD), including SCUD hunting, will need improved specific signature identification (data bases) for target weapon systems. This can be done via a number of signature specifics such as acoustic, seismic, thermal and RF emanations. There is a need to integrate such information data bases into U.S. weapons systems.

h. *MASINT support to Information Warfare.* Intelligence support to Information Warfare (IW) is a growing field. The potential utilities of MASINT systems need to be studied and evaluated for their IW potential.

F. "Although the CMO has the necessary legal authorities, it is not properly staffed commensurate with its responsibilities. Additionally, a fractured organizational structure provides little to no focused MASINT management, budgeting oversight, tasking control, or coordination of effort. This may potentially cause inefficient expenditures of resources and duplicative developments."

1) As stated earlier, MASINT as a discipline was created in 1986, with attendant start up of the MASINT Committee. Three directives provide guidance relative to the MASINT discipline. Specifically, the DCI Directive 2/11 gives CMO the authorities to provide for the "common concern (re: MASINT) on behalf of the Intelligence Community." The Department of Defense (DoD) Directive 5105.21, as amended, empowers the Defense Intelligence Agency (DIA) with the conduct of MASINT, and DoD Directive 5105.58 provides the CMO with authorities for MASINT within DIA. These directives proscribe specific responsibilities (for CMO) and MASINT management duties. Some of these duties include: providing direct and advisory tasking; developing MASINT policy; coordinating plans and architectures; and programming and budgeting. However, CMO's authority does not expressly extend to the use of CIA human intelligence assets for the collection and analysis of MASINT.

When first created, the CMO worked (organizationally) directly for the Director, DIA as the executive agency for MASINT. As a result of several DIA reorganizations, CMO's position within DIA has moved to within the Collections branch, organizationally subordinate to the National Military Intelligence Collection Center (NMICC). However, the GDIP Staff, which is

directly subordinate to the Director of Military Intelligence Staff and which is not directly in the CMO's chain of command, has a direct influence on the CMO's authorities. Specifically, the GDIP Manager, who is responsible for recommending GDIP resources for inclusion in or exclusion from the President's budget, orchestrates the budget process, allocates fiscal guidance, directs reductions and reallocations, and approves the GDIP budget. The GDIP Manager is assisted by three Defense Intelligence Functional Managers (FMs) for Collection, Processing, and Infrastructure. These FMs are charged with the preparation, supervision, and monitoring of GDIP programs and budgets within their areas of responsibility. The Director of the NMICC is also the GDIP FM for Collection. This puts the Collection FM and management staff directly above the CMO in the current organizational structure to represent MASINT and other disciplines/functions. This organizational construct limits CMO's actual influence over MASINT system development, tasking/operations, and programmatics. The MASINT Panel participants unanimously voiced opinions that the CMO is virtually powerless to direct and coordinate the MASINT effort. Additionally, CMO only has direct control over approximately 1/4 of the total MASINT funding[4]. The remainder is within the service and agency accounts. (It should be noted that much of this remainder pays for systems that not strictly MASINT systems or operations - therefore, much of this should not be the purview of the CMO.)

2) The CMO has true functional management over only those MASINT funds within the GDIP. Because CMO is a management organization, most of its funds are actually obligated by the Services or Agencies. For example, 84% of the GDIP MASINT funding is obligated by USAF (this equates to 30% of the USAF's GDIP TOA), and USAF provides 93% of the manpower[5]. These are important statistics in light of previous recommendations. Further, some respondents stated that CMO's direct authority over GDIP-only funds tends to focus CMO's efforts on GDIP issues. That is, CIAP and other (TIARA) programs do not get proper CMO attention because CMO does not have insight or leverage into these programs (the "Golden Rule" applies - "he who owns the gold rules"). Therefore, such programs may suffer a lack of community-wide direction. CMO needs insight into all "national" (CIAP) and "tactical" (TIARA) systems, missions and developments.

---

[4] MASINT Panel #2 and #3 discussions, and with CMO

[5] USAF MASINT briefing

3) The CMO's Mission Area Assessment identifies, as a critical need characteristic for future MASINT systems, a centralized/coordinated direction and oversight[6]. Under the current construct, the Services and Agencies have control of over 75% of all MASINT resources[7]. CMO has no direct control or oversight of these resources, rightfully so in some cases. But the fact remains, the CMO's ability to provide quality centralized management is hampered by organizational and budgetary barriers.

4) There is "no one in charge" of MASINT. An in-depth review of the MASINT "chain of command" reveals that it is difficult, if not impossible, to find a congruent chain of command for the MASINT "system of systems." That is, there is no continuous chain of responsibility flowing from the Director, DIA, through Director CMO to the Services/Agencies, to the collection systems, to the users and back. Despite the official DCI and DoD responsibilities and authorities assigned to the CMO, very little authority is actually applied in reality. This can be directly attributed to the fractured chain of command, limited CMO manning, and organizational construct under DIA denies CMO from providing a real community leadership role. CMO must actually assume the authorities (with additional billets described later) which it has been charged.

5) The Director, DIA -- not the Director, CMO -- is the real spokesman for MASINT at the Military Intelligence Board (MIB). This contrasts unfavorably with the Director, NSA and the Director, CIO, who are the (logical) spokespersons for their technical disciplines. The panel voiced concern that the Director, DIA is often forced to "choose" between MASINT issues and all other issues without having the technical expertise in the MASINT area. As an example, although budget cuts are worked in a formal process, MASINT R&D is considered by some as the GDIP budget's "soft underbelly," liable to be the first to take funding cuts (before, say, operational systems or manpower billets). It was acknowledged that some of the R&D cuts are due to poor execution of funds -- although execution rate determinates can be misleading. Nonetheless, CMO should have the real voice in MASINT matters to ensure that balanced, well-considered, logical decisions are made.

---

[6] MASINT 2010, Planning the U.S. MASINT System for the 21st Century

[7] MASINT panel #2 and #3, discussion with acting Director, CMO, Mr. Jim Fahnestock

6) With specific regard to the budgeting process, because the DIA GDIP Management Staff has significant authority in the current organizational structure over CMO, some respondents criticized that policy decisions often that do not reflect the professional thinking within the CMO. Additionally, since DIA is not an acquisition organization, CMO must transfer allocated funds to the services to work specific technology issues. This is done through the DIA comptroller. The process is slow and cumbersome, and does not provide the CMO the flexibility they need to ensure thoughtful technologies and reactive operations. Finally, because CMO's R&D budget must use the GDIP budgeting accounting process, obligation rates often lag behind the established "norms." Accordingly, these funds can be easily targeted for reduction even though their need is real.

7) Because of prior position cuts, until very recently, the CMO has been left without the necessary leadership (General officer or SES-level) that has the real authority to coordinate the MASINT community.

8) Based on panel respondent estimates, the CMO is understaffed, both in real terms based on current billets authorizations, and based on real need. Currently, the CMO is authorized 30 DIA billets -- 27 of which are filled; 6 CIA billets -- 5 of which are filled; 2 each Army and Navy billets - none of which are filled; 1 Air Force SES position -- the individual for this position was just recently hired; and 15 officer billets for the Consolidated MASINT Technical Collection Office (CMTCO) -- 14 of which are filled.)[8] Although a specific number needs refined analysis, several respondents discussed numbers of approximately 75-100 authorized CMO billets as being more in line with the tasked mission of the office. The current limitation of people relegates the CMO into an organization that is reactive in nature and "bound by the in-box." Additionally, CMO is not manned or postured to do material development. This development, in most cases, should be, and remains, the purview of the Services and Agencies. However, CMO should have oversight and coordination authorities for these programs. *Additionally, partly because of size and IC organizational structure, CMO is not aware of all MASINT-related programs conducted throughout the USG.* This is particularly true of multi-, hyper- and ultra-spectral sensing being pursued by various agencies.

[8] CMO figures.

9) The MASINT Committee and its subcommittees (which predate the CMO) exist primarily as a means of cross-flowing information between agencies and services. This committee is analogous to the SIGINT committee. Several participants questioned whether these committees (and subcommittees) are only necessary because CMO is not properly sized/staffed to meet its responsibilities[9]. However, a number of respondents stated these committees are extremely useful and should be maintained.

Findings/Recommendations

10) The Director, Central MASINT Office has the necessary legal authority to carry out the functions of a coordinated MASINT program. *However, because of a lack of personnel, grade and organizational structure, the Director, CMO does not have the real authority to carry out his/her responsibilities.* To ensure community-wide coordination of efforts, **CMO's charter under DCID 2/11-1 should specifically include the management oversight of all MASINT budget builds including CIA MASINT programs. This charter should also provide the Director, CMO the authority to "determine" the systems are or can be a MASINT contributors.** This would be to determine what systems could provide MASINT collection, and which could be logically managed within the MASINT program." This CMO authority concept may not be well received by the Services and Agencies, but is actually CMO's assigned task today.

11) **The Director of CMO needs to be a General Officer or SES-level position, with not only the statutory or executive order authority to be the spokesman for, but the real authority for MASINT, as is the Director, NSA for SIGINT.** The Director, DIA has recently hired a new SES as the Director, CMO. As of the writing of this report, any new titles/responsibilities/authorities to be granted this person are unknown. However, **the Director CMO, needs to be a permanent member of the MIB, NFIB and other senior DCI and DoD boards/panels as the representative for MASINT. His authority to establish MASINT community direction, standards, etc, should be on par with those of Director, NSA and Director, CIO (or the new NIMA). Director, CMO should also be a formal member of a senior steering committee that can vet MASINT issues applicable to the entire IC. (The *Intelligence Community Management* staff study recommends a construct for this to occur.)**

---

[9] MASINT panels 1, 2, and 3 and personal interviews.

12) **A MASINT management reorganization will be painful, but is necessary to ensure the viability of this critical future discipline. Such a reorganization should focus on joint units, offices, and organizations.** Such an organization should be within the TCA (see the *Intelligence Community Management* staff study). Specifically, MASINT management requires a "stand alone" capability like that of NSA - though all would agree, not the size. This should requires the equivalent of a U.S. MASINT System (USMS) like the U.S. SIGINT System or the U.S. Imagery System. **If there is no consolidation of the IC structure (i.e. a TCA) the CMO may need to be an organization independent of the DIA structure, but not necessarily independent of the Director, DIA.** For "care and feeding" purposes, the CMO can continue to exist within DIA, but must be an organization that reports directly to the Director, DIA, not the staff elements of DIA. Additionally, the CMO must have the authority to use existing (DIA) budgeting organizations (on an "outsourcing basis") to facilitate their obligation and transfer of funds as necessary. CMO could also be organized outside of DIA directly responsible to the Assistant Secretary of Defense, Command Control Communications and Intelligence. In either case, CMO needs to be responsible for all USG MASINT efforts (just like NSA is for SIGINT), and responsible to the DCI and SECDEF for satisfaction of MASINT information needs. In either case, the CMO must be given the real authority to take on the responsibilities laid out in existing charter.

13) **The CMO should be given the NSA-equivalent of the "SIGINT seal of approval."** (Under the TCA construct, this becomes a mute issue.) That is, CMO should be given a U.S. MASINT System (USMS) lead status with the ability to provide real guidance relative to programming, research and development, standards, tasking and operations. CMO should have more authority over service and agency developments and acquisitions (this should be a chairman of the board construct). This is not to undermine service/agency Title 10 authorities, but rather to provide a coordinated approach to resource expenditures. Again, this may not be well received by the services/agencies, but is actually CMO's assigned task today. **In conjunction with, and through the authority of the DDCI/CM's Infrastructure Support Organization (ISO), the CMO should establish MASINT system standards, with the services/agencies (the consolidated NRO) developing the material solutions.**

14) **Increase the size of the CMO. A specific number needs further analysis, however, respondents argue that a staff of at least 75-100 people is needed.** This number is based on an independent (e.g. no TCA) organization. Refined numbers for a division within the TCA will have to be determined. However, a TBD percentage of these billets should be military, with the services providing their experts to the organization. In the joint environment, the Director, CMO needs to facilitate the "cross-pollination" of services,

organizations, and agencies to ensure the long term needs of customers can best be satisfied. **Additionally, the CMO should have representatives assigned to the theater CINCs just as does NSA, DoD HUMINT, etc.**

15) **The role of the MASINT Committee should be further reviewed for adequacy/need.** Most study participants voiced a good deal of support for the MASINT Committee, stating that it provides a useful forum for the Agencies and Services to voice their concerns, opinions and positions as (CMO) policy decisions are developed. They believe this allows for infusion of some much needed objectivity into the MASINT decision process. However, there is a question of what the Committee's true charter is, particularly when viewed in the light of a stronger, more robust (also read: joint) CMO. There is no readily apparent savings or added value to dissolving the MASINT Committee, but the committee construct as a whole should be viewed for future relevancy.

16) **CMO must be able to state and maintain the necessary management positions (both popular and unpopular) relative to MASINT budget/programmatic recommendations and decisions. Such decision must be further incorporated within the CMS budget process (again, see the *Intelligence Community Management* staff study for further discussion).** Such coordinated budgeting can only happen if CMO is given and takes more direct control of the entire MASINT effort from budget through policy formulation.

Additional Thoughts

A. MASINT is a science-intensive discipline. Its one true characteristic is the need for practitioners well-versed in the broad range of physical and electrical sciences. These people cannot be honed from military service schools in one or two years. These people need to come from academia fresh with the scientific knowledge from experimentation and research. Nor can they continue to be "proficient" in their areas of expertise if they are maintained in government employ for an entire career. Such scientists must have portability. That is, they must be able to leave government employment and rejoin the ranks of academics in order to maintain their scientific knowledge. *The IC needs the personnel equivalent of commercial off-the-shelf technology (COTS).* **As part of the overall IC management initiatives, we discussed examining the feasibility of pursuing trial personnel management programs that provide incentives to recruit the necessary scientific experts for the IC's needs. Such programs need to be pursued with the full understanding that such experts may not spend a 20-30 year career in government employment. The Committee recognizes the magnitude of such a proposal, and stops short of attempting to enact this recommendation into law. However, the we believe plans, such as limited**

government pensions, movement of private pensions and savings plans into (and out of) the federal retirement plans, bonuses, etc., hold the promise of helping to ensure the Community can retain these experts for national service. We also believe there is a need to address the issue of being able to rehire retired military experts. Although costly, the returns in terms scientific knowledge would be well worth the investment.

B. For intelligence collection/support systems, there is a continuum that runs from those systems that provide pure intelligence collection and those that provide pure operational (i.e., SMO) support. In reality, all U.S. IC systems fall within the two extremes. There is a need to "plot" where individual systems fall, determine the IC strengths, its weaknesses (the holes) and use existing systems to cover the holes before setting off to build new systems or capabilities.

C. The intent of this report is not to "oversell" MASINT, but rather to call attention to some areas of concern, weakness, and, in fact, strengths. MASINT is not the most critical intelligence source for U.S. customers today. However, for any one particular incident or collection opportunity, no discipline always is. True all-source collection and analysis is critical. This report does try to emphasize that MASINT is a critical discipline that has the unique potential of being more so in the future. MASINT provides information that other sources cannot. This is not to say it is specifically a niche field, but can satisfy niche requirements.

D. The group identified (via various inputs) some recurring thoughts that would identify the MASINT system's greatest needs. These deserve reiterating:

- Educate people on what MASINT is and is not.

- MASINT can be used for immediate battlefield survival (tactical support).

- MASINT information is critical for national information needs (national survival) by providing information on the weapons of mass destruction and chemical and biological proliferation/use. There is a need to more clearly tie CMO's structure into the "national" (CIA) structure.

- Smart/brilliant weapons will, increasingly, depend on MASINT information.

- MASINT development must be focused on sensor to shooter and sensor to seeker head.

- MASINT provides the potential for unambiguous discrimination for identification of friend and foe (for preventing fratricide).

- Underground targets will be a future because of U.S. successes in DESERT STORM. This will add to the importance of MASINT exploitation.

- Requirements: there is a need for a "National MASINT Requirements Tasking Center" similar to the National HUMINT Requirements Tasking Center (NHRTC)."

- The services are justifiably concerned that any management/organizational changes may adversely affect warfighting capabilities. Any changes resulting from *IC-21* must factor those concerns, and a proper balance of centralized management/coordination versus operational needs must be found.

- There is absolute need for tasking and planning interactions between all players for all planning, R&D, system development, tasking, employment, etc.

- There needs to be a joint collection manager MOS/AFSC within the services, or, at a minimum, there needs to be an effective training block/course for all personnel assigned to work in collection management positions. How can we develop an JCMT without it?

Conclusion

There are a number of varied thoughts relative to the future of MASINT. Whether it remains a specifically-named intelligence discipline or not is less important than ensuring the viability of the technically and scientifically derived information from the many collection sources. User knowledge and insight as to what the MASINT product can provide for the future battlefield or for national objectives is imperative. Strong leadership is necessary to steer this "intelligence discipline of the future" into the next century.

COLLECTION: LAUNCH

Executive Summary

Spaceborne collection assets are useless if they cannot be put into orbit. Hence, launch vehicles will remain a critical component of the US intelligence collection architecture. Titan IV, the primary launch vehicle used by the Intelligence Community (IC), is prohibitively expensive. In order to meet the needs of all users, the US needs to move to simple, reliable, affordable launch vehicles. Though we believe the US must ultimately develop a new launch vehicle, interim solutions require the infusion of new ways of doing business and decreasing the IC's reliance on the Titan IV. The following recommendations reflect this approach.

- If technically feasible, all IC payloads should be taken off of the Titan IV. No Titan IVs should be purchased by the IC after the 1997 buy, and even that should be reconsidered.

- The U.S. should examine the viability of advanced technologies to reduce the size of satellites.

- The Air Force should modify its Evolved Expendable Launch Vehicle (EELV) program to focus solely on the heavy lift problem. The US government should take advantage of the Medium Launch Vehicle (MLV) competition between McDonnell Douglas and Lockheed Martin in order to keep MLV costs low.

- All IC payloads should move to the "ship and shoot" approach (i.e., payloads arrive at the launch site ready for launch, with no on-site assembly, testing, etc).

- Future IC payloads should conform to the standard interface of the launch vehicle. IC MLV class payloads should be compatible with both the Atlas IIAS/R and the Delta 3.

COLLECTION: LAUNCH

Launch vehicles are, and will remain, a crucial component of the US space architecture, especially in support of the Intelligence Community. Numerous government studies have espoused the criticality of our space transportation system to the US's assured access to space and have enumerated the many problems plaguing the launch vehicle community (LVC). Yet, nothing has come of these studies but piles of paper. No one has been able to push the solution forward for the real issue the LVC faces: the requirement for simple, reliable, and affordable launch vehicles. Though many organizations have tried, all previous efforts to build a new launcher have failed (ALS, NLS, Spacelifter, etc.) because the US Government (USG) tried to procure these systems doing business as usual. Costs grew substantially and programs were cancelled. The Intelligence Community (IC) is particularly vulnerable to the vagaries of the LVC. Because IC payloads are launched to support national security interests, required launch costs have been paid, regardless of how exorbitant. However, this climate is changing, mainly due to the current austere budget environment. With many of the IC payloads being scaled back or downsized to save costs, it is time to take a serious look at the LVC and decide if it is providing what we need to support intelligence requirements for the 21st century.

- **FINDING: Launch vehicles will remain a critical component of the U.S. intelligence collection architecture.**

In recent years, the IC has mainly been concerned with the Titan IV (TIV) launch vehicle and, in fact, the IC has been the main driver behind the need for a heavy lift capability because of the size of its payloads. The TIV has become the workhorse of the Community since (and because of) the Space Shuttle Challenger accident. It is the only US vehicle (besides the Space Shuttle) capable of providing a heavy lift capability. The TIV, along with the rest of the United States' launch vehicles, is based upon 1950's ICBM technology. ICBM developments were not optimized for low-cost production and simple, streamlined operations. These missiles were designed in the shortest time possible and built with the emphasis on maximizing performance (i.e., to carry the largest warhead possible) while minimizing the weight of the missile. Thus, very little design margin was allowed to keep the weight of the ICBM low. The Atlas launch vehicle is a perfect example of this. The structural walls of the Atlas missile's propellant tanks (and consequently, those of the Atlas launch vehicle) cannot stand up by themselves because the tanks' walls are extremely thin to save on weight. They must be internally pressurized for structural stability; otherwise, they implode. Hence, it is no wonder that our current stable of launch vehicles is not optimized for cost efficiency, robustness of design, and short operational timelines. Further, no matter how many times we upgrade these systems, their complex designs will never allow for ease of operations, low cost and maximum reliability. There is only so much that can be done with these legacy systems.

- **FINDING: The US needs simple, reliable, affordable launch vehicles. The Titan IV launch vehicle is not the best means of ensuring a viable 21st century collection architecture. Other options -- such as new launch vehicles and changes in satellite design -- must be pursued.**

The majority of IC payloads use the TIV. It is extremely expensive, unreliable, non-responsive, and pollutes the environment. It is definitely NOT the launch vehicle of the 21st century. The IC has four options to solve the above problems: 1) lighten the spacecraft so they can fly on a Medium Launch Vehicle (MLV); 2) perform product improvements to the TIV to increase reliability, improve responsiveness, and decrease cost; 3) hope the Evolved Expendable Launch Vehicle (EELV) program is successful at decreasing costs; or 4) develop a new launch vehicle.

- **FINDING: The Titan IV launch vehicle is prohibitively expensive.**

Though we believe that, ultimately, the country must make the investment in a new launch vehicle as stated in Option 4, we must deal with the realities of today. Also, as stated earlier, there appears to be very little that can be done in the form of upgrades to increase substantially reliability and to decrease costs for these legacy systems. Therefore, we recommend a combination of Options 1 and 3. The IC should reduce its payloads in weight and size to be compatible with the MLV class of boosters, at a minimum, but should strive, using advanced technologies, to attain the smallest satellite size and weight possible. We believe, with perhaps the exception of one program, that all current payloads that use the TIV can be downsized with no degradation in performance. This will drastically reduce launch costs for these programs.

- **RECOMMENDATION: If technically feasible, all IC payloads should be taken off of the Titan IV.**

Regarding EELV, we believe the Air Force should modify its program to focus solely on the heavy lift problem. Until it is ascertained whether the remaining IC program can be downsized to a MLV class booster, we must protect a heavy lift capability. However, MLV costs are already at the cost goals of EELV and both Lockheed Martin and McDonnell Douglas have committed to a MLV program, regardless of whether EELV lives or dies. This is based upon their forecasts for the commercial market. Hence, the USG should use this competition to its advantage and use both MLV programs, instead of locking itself into one contractor team as EELV proposes. Where is the incentive for the contractor to be low cost when it has a monopoly on the USG market? Allowing this MLV competition to continue would allow lower prices to be obtained and would provide a responsive backup capability if enough foresight went into the redesign of the new IC satellites. The new EELV program should mandate that the heavy lift vehicle be a derivative of the MLV programs so that economy of scale will be preserved (especially if the IC is left with

only one program requiring heavy lift). Several EELV contractors are already designing their programs in this way. There are some who predict that eventually there will be a commercial market for a heavy lift vehicle, based on the continuing trend of commercial communications satellites to grow larger. However, based on IC requirements, we do not have the luxury to wait and see if the commercial market will help to drive heavy lift costs down.

- **RECOMMENDATION: The Air Force should modify its EELV program to focus solely on the heavy lift problem. The U.S. government should take advantage of the Medium Launch Vehicle (MLV) competition between Lockheed Martin and McDonnell Douglas in order to keep MLV costs low.**

We applaud the IC in its current efforts to downsize its new spacecraft programs. Because these programs are entering a redesign phase, now is the opportune time to address launch responsiveness issues. The IC should require that these new spacecraft be designed in accordance with the "ship and shoot" philosophy, i.e., the spacecraft arrives at the launch pad ready for launch. No final assembly should be allowed on-pad nor should prolonged testing. Off-line processing and encapsulation need to become the norm, not the exception. This will help streamline operations at the launch pad, allowing for quicker launch turn-arounds. The IC should also mandate that its spacecraft use the standard launch vehicle interface that is available. This will allow spacecraft to be interchangeable on the booster (and between different boosters) should a problem develop with a payload (or a booster). This, too, will help to streamline operations and reduce costly payload-unique designs.

The ability for the IC to choose between an Atlas or a Delta launch vehicle for a MLV is now a reality because McDonnell Douglas has committed to the Delta 3. The Delta 3 will be comparable to the Atlas IIAS. The IC should require that all of its new spacecraft be designed to both launch vehicles' dynamic environments and loads. Hence, their launch flexibility will improve dramatically. It is only through implementation of these concepts that space can truly be "operationalized." Unfortunately, business as usual routinely has satellite program offices forcing the launch vehicle to customize its interface, versus the satellite adhering to the standard interface. This will only be changed if direction comes down from the top. The IC is in a perfect position to mandate these approaches and should do so immediately.

- **RECOMMENDATION: All IC payloads, during their current redesign phase, should incorporate the "ship and shoot" approach (i.e., payloads arrive at the launch site ready for launch, with no on-site assembly, testing, etc.).**

- **RECOMMENDATION: All IC payloads, during their current redesign phase, should conform to the standard interface of the launch vehicle. NRO MLV class payloads should be compatible with both the Atlas IIAS/R and the Delta 3.**

Not all IC programs have been as enthusiastic about embracing new technology and lighter weight materials. Their rationale was based on the economies of scale for the TIV program. If the IC pulled all of their spacecraft off of the TIV except for one program, the costs become prohibitively expensive for that remaining program. That does not mean, however, that we should continue to pay three times as much for launch vehicles for other programs (not to mention foregoing the cheaper satellite costs) to save the perception that the TIV program is affordable. Perhaps the cost savings would be eaten up by the TIV inefficiencies, but it might provide the impetus to devise new ways of downsizing the remaining heavy lift program, so it too could be taken off of the TIV, and provide more support to the heavy lift EELV program (i.e. with only one satellite requiring heavy lift, we need a more cost effective means of providing it). We have embraced a serious and timely examination of small satellite technology and believe that much smaller satellites can perform some, if not all, IC missions, with improved performance and flexibility. These new satellites could potentially use the small launch vehicle (SLV) class of boosters.

This SLV class of boosters includes the Lockheed Martin Launch Vehicle (LLV) and Orbital Sciences Taurus vehicle. We must mention some of the development problems this class of boosters is experiencing. LLV has had one failure out of one launch attempt and Taurus has had one success out of one launch (though its sister program, Pegasus, has had numerous failures and has yet to become truly operational, casting doubt on all of Orbital's launch vehicle programs). Though these boosters have had their share of problems, both companies have enormous incentive to make these programs viable from both a cost and reliability point of view. Both companies have commercial satellite programs that must fly on their own respective small launch vehicles. Hence, these companies must ensure that their launch vehicles will perform reliably and take their payloads into orbit. We believe these market forces will provide the impetus required to make these programs operational. If this does not occur, MLVs can always be used, albeit at greater cost (though still much cheaper than the TIV).

The remaining heavy lift program presents the IC with a major dilemma. The Air Force has no current plans to continue use of the TIV for Department of Defense (DoD) payloads past the follow-on buy scheduled for 1997. If all other programs are taken off of the TIV, the IC will have the only remaining program using this launch vehicle. Regardless of the number of programs it keeps on the TIV, the IC could very well be forced to pick up the whole tab for the TIV program, based on the Air Force's decision (though, at present, the Air Force has said this will not happen). This would be an increase the NFIP could not absorb. The IC, as a part of the aforementioned follow-on buy, will have procured TIVs for all of its approved programs. Production of these TIVs will be completed by 2000. It could be many years before the next TIV launch vehicle is needed. Thus, a major decision is needed in 2000 on whether or not to procure more IC TIVs.

We believe the IC should not purchase any more TIVs after the 1997 buy and that even this buy should be reconsidered. If the IC goes ahead with the 1997 buy, it will have bought, by 2000, all of the TIVs it needs for its approved programs, and then some. As part of the initial block buy, at least two TIVs were procured for spacecraft that have since been cancelled. There may be more TIVs available if other programs discussed earlier are downsized. Thus, the IC has a surplus of TIV vehicles. Based on new designs implemented by Lockheed Martin, a satellite program is not locked into a specific TIV configuration but can use any TIV vehicle. This greatly increases the IC's flexibility in using its surplus TIVs. (These surplus vehicles could be used for the remaining heavy lift program to protect a launch capability if the heavy lift portion of EELV cannot support this program.) Therefore, there is no need for the IC to procure more TIVs, including the 1997 buy, other than protection of the industrial base.

If the IC decides to buy more TIVs to keep the production line open, it will, in essence, entail a IC commitment to the TIV vehicle as the heavy lift benchmark for the next two decades, based upon satellite design timelines. In other words, the IC will be buying launch vehicles for satellites that will not fly for years. Because the most cost effective time to switch launch vehicles is between block buys, the IC will be saddled with the TIV for another 20 years. As stated above, we believe this is the wrong direction to take. Hence, no more TIVs should be procured by the IC.

- **RECOMMENDATION: No Titan IVs should be purchased by the IC after the 1997 buy, and even that should be reconsidered.**

To solve the particular problem of the remaining heavy lift program, R&D should be increased in the area of advanced technologies to support reducing the weight and size of the spacecraft. Alternate methods of performing this mission should also be pursued with increased, objective vigor (at a minimum as a part of the IC's Small Satellite Office's downsizing studies). If neither of these attempts at downsizing succeed, the IC will obviously be left with a requirement for a heavy lift capability but

at an extremely low launch rate. Thus, again, increased support needs to be given to EELV to ensure that the heavy lift derivative is closely tied to its MLV brethren. This is the only way that a heavy lift capability will be made affordable.

- **RECOMMENDATION: The U.S. should examine the viability of advanced technologies to reduce the size of satellites.**

In summary, the IC should attempt to downsize its spacecraft to eliminate the need for the TIV. We believe this can be achieved in all programs save perhaps one. R&D should be increased in technologies that have the potential to help the remaining program reduce its weight and size comparable to the capability of the MLV class of boosters (at a minimum). The IC should also mandate, for its programs going through a redesign phase, that they adhere to the standard launch vehicle interface and incorporate a "ship and shoot" approach. Finally, the Air Force should be encouraged to redirect their EELV program to focus solely on the heavy lift problem while demanding that the heavy lift vehicle be based upon a MLV derivative. Thus, if the IC's remaining program cannot be downsized, then EELV must provide a more cost effective heavy lift capability than the current TIV program. It is only in this way that the IC will be able to rely on affordable, assured access to space for its payloads in the 21st century.

CLANDESTINE SERVICE

Executive Summary

The purpose of this study is to present ideas about the future roles, organization, and management of a clandestine service as they were developed by the Study Group in the course of its "Intelligence Community in the 21st Century" *(IC21)* study. The body of the paper consists of explications of twelve principal "findings" concerning this clandestine service. Some of these findings represent radical departures from the *status quo*. Others simply reaffirm and revalidate existing arrangements that have been under question.

While this study stands on its own, its observations and conclusions are compatible with the other *IC21* studies. Moreover, when looked at in the context of the Committee's examination of the Intelligence Community (IC) as a whole, the following findings and recommendations have been extracted from this study for inclusion in legislative proposals to reorganize and better direct the IC in the future:

Findings

- **The U.S. requires a clandestine service of the highest professional standards and competence.**

- **Clandestine collection must be focused principally on select, high priority national and military requirements.**

- **Yet, it is necessary to have at least a minimal clandestine presence in most countries (a "global presence") so as to maintain a broader base-line contingency capability and to respond to transnational collection requirements.**

- **Clandestine operations require an extraordinarily high level of management attention, expertise and coordination.**

Recommendations

- **There should be a single US clandestine service (the "Clandestine Service,") under the Director of Central Intelligence's (DCI) direct supervision.**

- **For intelligence collection tasking and requirements purposes, the Clandestine Service should respond to the regular community-wide collection management process.**

- **The Clandestine Service should be managed by a Director who is a career intelligence professional.**

- **The Clandestine Service should have a two-star professional military intelligence officer as a Deputy Director responsible for support to the military and for coordination, as appropriate, with the military services, regional commanders and the Office of the Secretary of Defense.**

- **The Clandestine Service should have organic to it the administrative and technical support mechanisms that are critical to its unique functions and essential to its success.**

- **The personnel system should ensure the recruitment of highly qualified junior employees, the development of talented clandestine operators and managers, and the aggressive removal of marginal and unsuitable employees.**

- **The military cadre of the Clandestine Service should consist of military clandestine operations officers having a viable military career track within that specialization and of the same high professional and personal qualifications as the civilian cadre.**

- **The DCI needs to reaffirm and reiterate throughout the IC, his designation of the Clandestine Service's role to lead the IC in its conduct of foreign clandestine operations, i.e., espionage, counterespionage, covert action and related intelligence liaison activities abroad.**

- **The Clandestine Service Chief of Station should act as the US government's on-site focal point for the deconfliction of all intelligence and law enforcement activities abroad with an appeals process functioning through the Ambassador and/or a Washington-based interagency mechanism.**

There are numerous other findings and recommendations within this study that will be pursued by the Committee in other ways, particularly through the annual authorization and regular intelligence oversight process.

CLANDESTINE SERVICE

Definition of Terms: "HUMINT" and "Clandestine Service"

The terms employed in this study reflect some of its findings. The most important example of this is the use of the terms "HUMINT" and "clandestine service." Originally, the Study Group had characterized this part of the *IC21* study as being about HUMINT. The term is, however, a particularly ambiguous one, the use of which frequently masks if not perpetuates intellectual sloppiness. Properly speaking, HUMINT refers to a category of intelligence, that which is reported by a government information collector who has obtained it either directly or indirectly from a human source.[1] As such, the term hardly begins to encompass the subject under consideration: the proper mission, management and organization of the entity or entities responsible for foreign clandestine intelligence operations (i.e., espionage, counterespionage, covert action and related foreign liaison activities). Such an entity is a "clandestine service."

A clandestine service does much more than simply collect "HUMINT" clandestinely, that is secretly exploit agents for the purpose of collecting intelligence. A clandestine service also works in liaison with other spy services to run all types of operations; it taps telephones and installs listening devices; it breaks into or otherwise gains access to the contents of secured facilities, safes, and computers; it steals, compromises, and influences foreign cryptographic capabilities so as to make them exploitable by US SIGINT; it protects its operations and defends the government from other intelligence services by engaging in a variety of counterespionage activities, including the aggressive use of double agents and penetrations of foreign services; and it clandestinely emplaces and services secret SIGINT and MASINT sensors. It also has the capability of using its techniques and access to run programs at the

---

[1]The term HUMINT was coined as a contraction of "human intelligence," a category of intelligence meant to contrast with the varieties of technical intelligence known as SIGINT (signals intelligence), IMINT (imagery intelligence), and MASINT (measurements and signatures intelligence). As usually employed now, any intelligence coming from a meeting with a human source - clandestine or overt - can be categorized as HUMINT. Nonetheless, overt HUMINT is also sometimes categorized as a type of open source intelligence, which is now in some corners called OSINT. To confuse matters further, any intelligence disseminated by the CIA's Directorate of Operations, even that coming from several of the traditional types of technical operations (e.g., from teletaps and audio operations) is sometimes lumped into the HUMINT category. Also, the Department of Defense (DoD) sometimes calls the reporting coming from the direct observation of a US intelligence reporter "HUMINT."

President's direction to influence foreign governments and developments, that is, "covert action."[2] The unifying aspect of these activities is not some connection to HUMINT; rather, they are highly diverse but interdependent activities that are best conducted by a clandestine service. The terms "HUMINT service" and "clandestine service" can be used interchangeably only in ignorance or with a willful disregard for the actual meaning of the words.

A final note on the use of the term "clandestine service." When referring specifically to an existing clandestine service, such as the CIA's Directorate of Operations (DO) or the clandestine element of the DoD's Defense HUMINT Service (DHS), this is done so by name. In discussing an ideal or future organization performing those missions, we have used the term "Clandestine Service" or CS as a proper noun.

Background: Clandestine Operations and a Clandestine Service -- How Important Are They? Do We Need Them? Will We Need Them?

There is no more beleaguered element of the Intelligence Community than the clandestine service -- the organization currently known as the CIA's Directorate of Operations (DO).[3] It has been the subject of ceaseless critical scrutiny and even vilification from the press and more than occasionally from Congress since the

---

[2]This study will concentrate on the intelligence collection aspects of clandestine operations. It is this study's assumption that any serious examination of covert action will conclude that it would be inefficient and unwise to separate covert action from clandestine intelligence activities such as was attempted and abandoned in the early years of the CIA. Since 1952, the CIA's clandestine service (the Directorate of Operations and its predecessor organization, the Directorate of Plans) has been responsible for the full panoply of covert action activities. These range from running agents of influence who can clandestinely influence a foreign government's policies to executing clandestine or, at the least, "plausibly deniable" paramilitary operations meant to overthrow or harass foreign regimes. Covert action also frequently involves the exploitation of covert or clandestine cooperative intelligence relationships with foreign countries to further US positions in a type of quiet diplomacy. Experience has shown that the quality of a covert action is usually directly proportional to the quality of intelligence collection because the best agents of influence frequently have the best access to intelligence and vice versa.

[3]For the purposes of discussion in this section of the study, we will concentrate on the DO. Although the newly created Defense HUMINT Service of the Department of Defense consolidates most military clandestine operations, it is as yet an infant organization running fewer operations globally than does the CIA in many countries.

Congressional hearings of 1975 and most recently since the arrest of Aldrich Ames, a DO employee, in February 1994 as a Soviet (and later, Russian) agent.

The tenor of much of the recent reporting is exemplified by a statement in the *U.S. News and World Report* that the DO is at the center of a system of "incompetence, corruption, cover-ups, and ... failures."[4] In Congress, there has been no reluctance on the part of some to make public accusations of DO malfeasance, ineptitude and even illegality. Recent examples are false charges of DO involvement with assassinations in Guatemala and of costing taxpayers billions of dollars by passing on Soviet/Russian disinformation that was used to justify supposedly unnecessary US defense programs. The political and editorial mood is such that charges of this sort, although they frequently prove to be overstated if not outright wrong, find immediate acceptance and make the public even more receptive to subsequent further "revelations." It would appear that the the current DCI, John Deutch, has been, at least to some degree, influenced by these stories and allegations, since he has publicly lamented the DO's "tremendous deficiencies" and reportedly put on his daily calendar a standing objective of "reinventing the DO."

Ironically, however, the DO of the last few years appears to be at least as and possibly more successful than it ever has been. It has made significant advances in penetrating the great majority of hard target countries and a wide variety of terrorist and proliferation organizations. It has dramatically redefined and focused its activities on high-priority national intelligence issues. Its Office of Military Affairs, under an Assistant Deputy Director of Operations for Military Affairs (ADDO/MA) (created after Desert Storm had shown weakness in support to the military), received strong kudos from its military customers. In response to a perceived need to tighten up its bureaucracy, the DO has also dramatically reduced personnel (to the point that it is two years ahead of its Congressionally-mandated goals), closed down a sizable fraction of its stations and bases in the last four years, and drastically cut back on the number of personnel in the field. It has opened up some of its operations and brought in outside experts at an unprecedented level to the point that seniors from the Directorate of Intelligence, FBI, the military and DoD civilian organizations serve in positions up to and including the division chief level.

These positive assertions -- standing in such stark contrast with the negative general assessment that recent accusations have fed -- are sustained by what little objective data there is available to assess the relative value of the DO's product. The Committee is aware of three studies attempting to develop hard data on the utility of the intelligence produced by the intelligence disciplines: the Strategic Intelligence Review (SIR) process of 1994, a survey of *National Intelligence Daily* (NID) citations,

---

[4]John Walcott and Brian Duffy, "The CIA's Darkest Secret," *U.S. News and World Report*, 4 July 1994, p. 35.

and the 1995 Comprehensive Capabilities Review undertaken by the Community Management Staff.

The twelve SIRs prepared at the DCI's request and under the auspices of the National Intelligence Council in May 1994, identified 376 intelligence "needs" and rated the value of the contribution of the various intelligence disciplines (HUMINT, IMINT, SIGINT, MASINT, and open source) in meeting those needs. An example of such a need is "International terrorist organization X's plans to attack US persons, facilities, and interests." In aggregate, the SIRs clearly identify HUMINT as the most important source of intelligence for the subjects treated.[5] Specifically, HUMINT was judged to make a "critical" contribution towards 205 of the 376 intelligence needs identified. That is more than half again as much as the next greatest contributor (SIGINT) and more than twice that of the third (open source).

Within several important specific subject areas, HUMINT's contribution is particularly strong, such as in reporting on the transnational issues that are now among the highest priorities of the IC: terrorism, narcotics, proliferation, and international economics. In providing information on terrorism, HUMINT garnered the grade "of critical value" almost 75 percent of the time it was given. In narcotics, HUMINT was graded critical more than the other intelligence disciplines put together. In collecting critical intelligence on the proliferation of weapons of mass destruction and their delivery systems, HUMINT's contribution was over 40 percent. Finally, in international economics, its contribution was over one third. Similarly, in several more traditional areas of foreign political intelligence and regional developments, HUMINT was rated the most important source for covering the Near East, South Asia, Europe, and Africa. In summary, it would appear to be safe to conclude from the Reviews that what they term as HUMINT is unsurpassed as a source of critical intelligence to the national policymaker.[6]

Another effort at objectively assessing the usefulness of intelligence coming from the various collection disciplines is a study that was done of the intelligence sources used in the preparation of the NID for January 1993. Not surprisingly, open source and Department of State reporting were the most frequently cited sources of

---

[5]It must be noted that the Reviews are inconsistent in their use of the term HUMINT. Frequently they use it in exclusive reference to clandestine HUMINT and refer to overt collection as part of open source collection. Yet, in other instances it lumps clandestine and overt in the same "HUMINT" category.

[6]As is discussed under "Finding Four" of this study, the role of clandestine reporting is significantly more limited in supporting the tactical intelligence requirements of military commanders. This is most evident on a technologically sophisticated battlefield where technical intelligence collection techniques can be far more useful.

information. They were followed by the various types of intelligence reporting in the following order: DO reporting, SIGINT, imagery, and Defense Attaché reporting. By issue, the DO was the most important intelligence source in the areas of weapons proliferation, economic security, Europe, Africa, Latin America, terrorism, counternarcotics, and Somalia. Although this is, of itself, a good reflection of the value of the DO's product, it does not capture it all, since the NID does not typically reference much of the DO's best reporting that is disseminated only within highly restrictive "blue border" compartments.

Finally, in late 1995 the DCI's Community Management Staff (CMS) prepared a Comprehensive Capabilities Review that is probably the best effort yet at objectively assessing the collection capabilities of the various parts of the intelligence community. In this case, the CMS worked from the specific intelligence issues as categorized and prioritized by Presidential Decision Directive outlining intelligence priorities. In this review, too, clandestine operations elements had a strong showing. In the crisis capability category, the clandestine HUMINT collection capabilities were rated as being of approximately the same value as SIGINT. Against the category of transnational issues, the DO's capabilities were unquestionably the strongest in the intelligence community, being half again those assessed as belonging to SIGINT. Against "rogue" states and other top priority target countries, the DO played a secondary role to SIGINT. It is worth noting that in this review the assessment of the DO's production was only of its "HUMINT" reporting and did not include the reporting that results from the DO's clandestine technical operations.

The demonstrable value of CS reporting and its more than respectable showing in relation to other types of intelligence is further highlighted by its relative low-cost, except in comparison with open source collection: at a single digit percentage of the National Foreign Intelligence Program budget, clandestine operations cost a small fraction of what is spent on IMINT and an even smaller fraction of what is spent on SIGINT. This is not always understood and, in particular, is lost on the public. Even Roger Hilsman, a former intelligence officer, referred in a recent *Foreign Affairs* to the "enormous cost of fielding secret agents."[7] The fact is that US espionage under even the most sanguine projections has little prospect of ever costing more than a fraction of what is spent on technical intelligence collection programs.

Even if we accept the current value of a CS and its relatively low cost, the *IC21* study, of which this is part, is looking to the future. For that reason we must ask whether it will also be useful in the future. Although it is difficult to foresee the geopolitical situation of ten or fifteen years from now, there are several characteristics of good clandestine operations that point to their probably being particularly well-

---

[7]"Does the CIA Still Have a Role?" *Foreign Affairs 74*, no.5 (September/October 1995): 110.

suited to meet many post-Cold War national intelligence requirements. Although the details are much debated, the IC, the executive branch, and Congress are all in basic agreement that the most important intelligence requirements will fall in the following categories: the transnational issues of terrorism, narcotics, weapons proliferation, and economic competitiveness; hostile states; strategic threats; support to the military; and "hot spots." Six points are worth making here about how a good clandestine service can be of particular value in satisfying such requirements.

First, transnational issues involve the linkage of individual players around the globe operating in secret cooperation if not alliance. These are notoriously difficult targets for intelligence. But experience has shown that there are often weak links in such organizations and good clandestine operators are ingenious at locating and exploiting them. Thus, of all the intelligence collection techniques, clandestine operations have a comparative advantage in collecting on most transnational issues. The Strategic Intelligence Reviews of 1994 and the Comprehensive Capabilities Review of 1995 have amply documented this strength. Moreover, there is no reason to suspect the clandestine operator's capabilities will be less successful against these targets in the future. This judgment assumes that the clandestine service is not forced, for political reasons, to limit its ability to recruit and run agents inside the frequently unsavory circles and governments in which terrorist, narco-traffickers, proliferators and criminal elements operate.

Second, so long as there are humans at the controls of foreign governments making decisions in secret affecting our national security, clandestine operations will be important and effective in ferreting out the secrets. There is, of course, the intelligence truism that espionage is uniquely well-suited among the intelligence disciplines to discover plans, intentions, and deliberations. That opinion is complemented by the less understood, but equally true, argument that only a spy can actively delve for intelligence. Technical intelligence collection requires specific types of action on the part of the target--the visible movement of troops, discussions of plans over accessible communications links, the development of chemical compounds or biological forms that can be detected, and such. A spy, however, can even dig into the hypothetical to satisfy an intelligence consumer, as, for example, when a well placed agent in a foreign government is tasked to ask his leader, "What will we do if the US does x?" Clandestine operations can, in short, shake the intelligence apple from the tree where other intelligence collection techniques must wait for it to fall.

Third, the same global developments that are making intelligence collection less necessary in some cases -- the opening of previously closed societies, political and economic integration, and increasingly mobile and free populations -- are working to facilitate the clandestine operator's task of getting to the important secrets that do remain.

Fourth, counterintelligence will continue to be a challenge to the US so long as there are hostile intelligence services, and clandestine counterespionage operations (the running of penetrations of those services) has been and gives every indication of remaining the most important keyhole we will have in detecting hostile intelligence activities. The overwhelming majority of espionage cases opened by the Federal Bureau of Investigation over the last thirty years has come from information provided by human penetrations, most of them coming from the DO's large numbers of penetrations of foreign services. Notwithstanding new executive orders and Congressional interest in increasing interagency counterintelligence analysis, analytic successes will be extremely limited without the lead information and raw data originating from clandestine operations.

Fifth, the CS will continue to have tremendous potential to ensure the success of other intelligence collection disciplines. In particular, the CS will be called upon to continue its support of SIGINT. It is no surprise to those who understand cryptography to learn that most cryptographic systems in use are exploitable only if the codes are in some way compromised. Quite simply, brute computer attacks on codes are usually unsuccessful. Arguably, a clandestine service's greatest contribution to intelligence is the compromising of codes. The proliferation of sophisticated cryptographic systems ensures the growing importance of this role of the CS.

And sixth, the CS's unique ability to develop clandestine access to foreign facilities and locations will become increasingly crucial to the whole intelligence community, the SIGINT and MASINT disciplines in particular. This Committee has a strong record of supporting clandestine technical operations and, over the last few years, has been greatly encouraged and pleased with the development of those capabilities in the CIA in conjunction with other elements of the IC. The CS will undoubtedly continue to play an increasingly prominent role in helping technical collectors gain access to the media and materials they exploit.

In summary, we believe the importance of clandestine operations is greater than is usually recognized and that there are strong reasons to believe they will be both successful and appropriate in satisfying intelligence requirements in the future. That said, there remain numerous questions about how to define further what the CS of the future should do, what it should look like, and how it should operate. The "findings" that follow are meant to address some important aspects of those questions.

Finding #1: The Clandestine Service should be small and principally focused on select, high priority requirements to which it can make a unique contribution.

The current Deputy Director of the National Intelligence Council has advised the Committee that, from every corner, on every issue, we hear the consumers say, 'We need more HUMINT.'" The Committee has heard the same from almost every current and past senior consumer of intelligence it has consulted -- from National Security Advisors, Secretaries of State and Defense, and CINC's. None of them has ever said they wanted or could do with less. In this is recognizable the commonly held belief that human spies can best fulfill the greatest (and most challenging) need of the intelligence consumer, that is, **advance** knowledge of foreign developments, or, as it is more usually called: plans and intentions.

We share the belief that clandestine operations are frequently the best means of getting that type of intelligence, but are reluctant to embrace any call for an expanded CS. There is a strong case for better, not necessarily more, HUMINT. The reasons are several. Among them are that clandestine operations:

1) require a management and coordination process that, on a large scale, becomes cumbersome and bureaucratic;
2) require a tight focus for long term planning;
3) must overcome the human tendency of clandestine operators and managers to do that which is easiest rather than most important; and
4) involve an element of risk and potential for embarrassment greater than most intelligence activities.

First of all, a large organization running clandestine operations is prone to intense and byzantine bureaucratization, particularly in its headquarters element. A properly managed CS will be steeply pyramidical in its management structure. Unlike some SIGINT or IMINT activities, in which a first line manager may supervise ten, twenty, or more collectors and producers of intelligence, clandestine operations usually require a case officer/first line manager ratio of no more than three or four to one.

A typical station might have five clandestine operations officers including the Chief of Station (COS). The most time-consuming responsibility of the COS and his Deputy would usually be the supervision of the three junior officers typically on their first or second assignments. If a station is larger, branches will be formed so that oversight of the operations remains equally intense. At the headquarters, depending upon the sensitivity of the activity, any number of hierarchical levels may get involved with double-checking and, as required, approving the field's operational activities. In its most simple form, the operational chain of command at the headquarters is: a desk chief (usually in charge of a small country), a branch chief (in charge of several small or one large country), a division chief (in charge of a continent or geographic region),

and, ultimately, the director of the CS. Deputies to these various levels may or may not also get involved. Additionally, there are functional offices and staffs within the CS that must be consulted according to their charters or when their operational equities are involved.

For example, an operation in a European country to penetrate a Near-East based terrorist cell may involve: one or more of the desk, branch, and division level offices overseeing European operations; the Counterterrorism Center element responsible for operations around the world meant to penetrate the terrorist organization; desk, branch, or division offices overseeing the Near-East nationality of the terrorist in question; the counterintelligence office double-checking the *bona fides* of the source; an Office of Technical Services element responsible for providing and servicing covert communications equipment the source might use back in his home country; and the office responsible for providing the case officer with cover for his travels.

Despite innumerable ideas at streamlining this sort of process, most CS managers have concluded that they are largely unavoidable and that, in a small, focused organization, they actually serve to enhance the security and productivity of operations. Moreover, in a small CS, working only cases that meet a high operational threshold, such a process of double-checks and coordination can work surprisingly quickly and smoothly, usually within a day. Advances in office automation and communications should speed this process even more in the next decade. However, it is easy to see how a CS dealing with large numbers of marginal operations will have to build a large bureaucracy to handle the load, making the whole system sclerotic and unresponsive.

Second, clandestine collection requires long-term planning and a focus that come best to an organization forced to plan strategically the allocation of its scarce personnel resources. Access and capability are two central concerns for all intelligence collection managers. Some technical collection disciplines plan mostly to develop generic capabilities -- an imaging satellite that has a resolution of so many centimeters or a signals processor that can scan and select from some minimum number of channels. These capabilities are to some degree fungible -- sometimes by a simple change in the daily tasking or, somewhat less immediately, by shifting a satellite's orbit from over, say, Iran to North Korea. Clandestine operations managers must concentrate more on building target specific access, a process that, more often than not takes months if not years. Examples are: placing a non-official cover (NOC) officer or recruiting an agent in a company that can plausibly get close to a covert weapons proliferation conduit; finagling a way to get inside a terrorist safehouse to implant listening devices; or buying a house from which to mount a technical collection operation. Since clandestine collection is relatively unresponsive to quick changes in direction, it must keep a tight focus on its long-term objectives. Mistaken or unclear priorities result in an immediate loss of attention to more deserving issues as well as significant, lingering inefficiencies.

Third, some of the characteristics of clandestine operations work to reinforce the tendency of human nature to direct attention towards that which is most likely to succeed rather than that which, if successful, can yield the greatest benefit. This tendency can be difficult to detect and counter in a large CS since the sheer volume of activity can mask the lack of quality operations.

The raw material of clandestine operations is people. The challenge to leadership of a CS is in motivating these people to concentrate on the hardest objectives. This challenge is greatly increased by the fact that in the CS great successes are rare and failure is routine. Months of work can go into implanting a listening device in an office of a high-level diplomat from a "rogue" state who is close to his president, only to have him die and be replaced by a nonentity. Weekend after weekend can be spent attempting to win the confidence of an apparently disgruntled hostile intelligence officer, only to find out that he has been "dangled" before the case officer. Case officers can inflict on their families innumerable, inconvenient early morning walks in a park in the vain hope of being able to bump into and strike up a friendship with a targeted code clerk who is known to take his children for walks there on occasion. Frustrations can mount and the desire to succeed or, at least, sense forward motion also becomes more intense. Under such circumstances, the temptation is great to lower sights and work an easier but less important target. If given in to, this results in a system that measures success by the numbers of operations rather than their quality -- a charge that was frequently leveled against the DO, particularly in the 1980's when it was expanding in size. A small CS, under pressure to produce results against the hard targets and constantly forced to make hard choices on how to allocate limited human resources, is less likely to fall for this expedient.

Finally, although clandestine collection is frequently less expensive than some technical techniques, it tends to be much more politically sensitive. Moreover, with the disappearance of a Soviet or Communist threat, fewer and fewer friendly countries are willing to accept the presence of a free-wheeling US CS as part of the price of being allied with the US. Although this situation may change in the coming years as global dynamics change, there is no denying a complex calculus that must be done as part of the risk/gain analysis that is crucial to the responsible management of any

clandestine operation.[8] A small, focused CS is more likely to be careful in its application of this calculus.

Having made these arguments, it is only fair to note that the DO's current personnel resource plans more than meet the requirement that the CS be small. The degree to which the DO has already drawn down and refocused its personnel resources has gone almost totally unrecognized. Yet, the facts are stunning, even in an IC that is seeing significant continuing reductions in personnel across the board:

- ❒ Since 1990 the DO has reduced the number of "core HUMINT collectors" by over thirty percent.
- ❒ Since 1992 it has closed large numbers of stations and bases.
- ❒ Large stations have been, on average, reduced in size by over sixty percent.
- ❒ The number of deployed, officially covered case officers has been declining at an average rate of almost ten percent a year for the last several years.
- ❒ In overall personnel strength (including support staff), the DO has already met its Congressionally mandated FY 1998 personnel reduction goals.

We believe these changes have been, on balance, healthy for the DO and, barring significant changes in the international environment, current personnel levels are appropriate for the proper utilization and management of the CS into the next century. Although the CS of the future will be challenged by a growing demand from intelligence consumers for more clandestine collection, the proper response, in most cases, is to strive for better quality reporting and, as necessary, to reprioritize collection to satisfy the most important requirements, rather than to make a net increase in human resources to satisfy the requirements.

Along with the aggressive moves to draw down and redirect personnel resources, there has been for some time a move towards narrowing the focus of

---

[8]This calculus is frequently misstated even in the IC by those who would weigh the potential intelligence benefit from an operation against the cost of its **assumed** compromise. So, for example, one would ask, "Assuming this will be compromised and be used against us, is it worthwhile recruiting the army chief of staff in country X?" Needless to say, few operations would be justifiable under such a formulation. Similarly, no one would ever drive to a grocery store or to work if that action were being weighed against an assumed worse case scenario -- a fatal auto accident. The proper calculus is to weigh the potential intelligence benefit against the cost of a **realistically appraised possibility** of compromise.

clandestine operations to "operations that count." To do this, personnel resources in the DO have been redirected to increase attention to "hard" targets. There have been several "zero-based" reviews of the inventory of agents to terminate handling of those who do not materially advance efforts to penetrate hard or other high priority targets.

This finding is based on the "supply side" management of CS personnel resources as the surest way to limit clandestine operations to those operations satisfying truly important requirements uniquely amenable to its techniques. The "demand side," or "requirements" as they are called in the IC, also must be worked. All intelligence collectors are faced with intelligence requirements that massively overload the system. This is a long-standing problem that many collection managers and outside experts have identified as possibly the most persistent and troublesome of all those facing the IC. Fortunately, in the National HUMINT Requirements Tasking Center (NHRTC), set up in 1992 under the direction of the deputy Director for Operations (DDO) in his role as the National HUMINT Collection Manager, clandestine operations undergo the most rigorous, formal requirements vetting process in the community. (See the *IC21 Intelligence Requirements Process* staff study for further details.) The NHRTC measures requirements by importance and allocates them to the most appropriate, least risky collection mechanism available.[9] The rule of thumb is that clandestine capabilities are to be tasked with a requirement only when these capabilities are uniquely able to satisfy them and the requirement rises to a level justifying the risks that would be entailed. The CS seems to have in place already much of the requirements management process that the CS of the future will need.

Finding #2: The DCI needs to reaffirm and, as necessary, expand upon existing guidelines to ensure the role of the Clandestine Service in leading the Intelligence Community's conduct of foreign clandestine operations, i.e., espionage, counterespionage, covert action and related intelligence liaison activities abroad.

There are two parts to this finding. They build upon existing DCI and COS authorities.

---

[9]NHRTC's guidance is binding on the clandestine and overt HUMINT collection elements inside the IC, such as on the DO and the overt and clandestine elements of the Defense HUMINT Service. It is advisory in making its recommendations to the collection elements outside the community, such as to the Foreign Commercial Service of the Department of Commerce and in the Department of State embassy reporting program. NHRTC's effectiveness in validating and allocating requirements has been recognized and further improved by its also providing guidance for open source collection in the IC, such as by the Foreign Broadcast Information Service of the CIA's Directorate of Science and Technology.

First, the CS should have direct control of all US foreign clandestine operations, that is, those that have been defined in DCI Directives as espionage related. Those are, specifically, all intelligence activities "directed towards the acquisition of intelligence through clandestine methods." Clandestine operations are compartmented on a need-to-know basis. It is crucial that someone be cognizant of all operations in a country so as to deconflict, guide, rationalize and validate them. When this centralized oversight breaks down, there can be a needless waste of effort and, more importantly, compromises of operational security.

There are numerous examples that have been cited of the problems that have resulted when this principle is not understood or accepted by all parties. One US intelligence organization approaches a foreign target not knowing he has already been recruited by another US intelligence organization - or worse, not knowing that he has already been identified as working for a hostile foreign intelligence service. A non-resident US intelligence operative flies into town and meets his clandestine asset in a hotel that the COS knows to be under surveillance and audio monitoring by the host country. A US intelligence organization expends a great deal of effort to meet and recruit a target of apparent interest not knowing that the target's supervisor, an individual whose access far exceeds the target's, is already a US intelligence source. There is no shortage of such examples. There is also reason to be concerned over some of the proposed command and control structures that had been proposed for some of the clandestine operations of DHS. These appeared to have as their objective the circumvention of the COS's cognizance of the details necessary to "conduct and coordinate" liaison as outlined in DCI directives. These concerns have figured to some degree in the development of Finding Twelve of this study, recommending, in effect, a unified CS, jointly managing the operations of the DO and the DHS (which had itself been created to better manage diverse military intelligence operations).

The second part of this finding also revalidates and reinforces the existing guidelines directing that the local head of the CS, the COS, as the DCI's representative, be responsible for the conduct and coordination of all US government intelligence liaison activities in any way relating to espionage (that is, clandestine collection activities) and counterespionage. The designation of a single authority for the conduct and coordination of such activities makes sense in that it ensures intelligence policies towards a specific country are applied uniformly and minimizes the chance that one US intelligence channel is played off against others. It enables the Ambassador to have a single reliable point of reference for all intelligence activities. Additionally, it minimizes confusion on the part of the host country such as has occurred in some countries where the sudden warming of relations resulted in a rush of uncoordinated US initiatives to establish liaison relationships. The establishment in 1992 of the DCI's Special Representative for Foreign Intelligence Relationships has improved this situation, but there are still too many instances where there is less than total adherence to the current directive.

Finally, the CS of the future, if it is to continue as the President's main instrument for covert action, must also be responsible for the use of information warfare capabilities in situations other than war. Increasingly, covert action and offensive information warfare techniques are converging. The US government may wish in the future to employ some offensive information warfare capabilities that are principally resident in DoD and outside the CS as part of a covert action. In such cases, the President (through the DCI and CS) and Congress should exercise covert action-type control and oversight of those activities. To this end, the CS must play a more important role in influencing the development of these capabilities and ensuring their applicability to covert action requirements. An executive order to this effect should be promulgated and Congress advised if any legislative assistance is required.

Finding #3: Overseas Coordination of Intelligence and Law Enforcement - The Clandestine Service Chief of Station should act as the US government's on-site focal point for the deconfliction of all intelligence and law enforcement activities abroad with an appeals process functioning through the Chief of Mission and/or a Washington-based interagency mechanism. Also, without prohibiting or preempting law enforcement liaison activities, the Clandestine Service should have the authority to carry out liaison with any foreign intelligence and/or security entity of operational interest or utility.

As a corollary to Finding Two, there must also be a greater degree of coordination between law enforcement and intelligence overseas. Clandestine intelligence and law enforcement operations can easily run afoul of each other.[10] It is essential that there be a clearly understandable and practical mechanism to make sure this does not happen.

Terrorism, narcotics, weapons proliferation, and international criminal activities can be of interest to the intelligence or law enforcement communities or both. The techniques of greatest utility overseas also overlap. The CS's two most productive techniques -- unilateral clandestine agent operations and liaison with foreign security and intelligence services -- are also the two that are of greatest utility to the law enforcement community in its overseas activities. What complicates this is each community's penchant for keeping its activities secret from the other. In the case of the IC, it has concerns over protecting sources and methods. Those concerns are heightened by the potential of having those sources and methods exposed if intelligence provided to law enforcement agencies becomes subject to "discovery." Law enforcement agencies, on their part, are anxious not to jeopardize ongoing

---

[10]The other major issue between law enforcement and intelligence is the use of intelligence information and capabilities for law enforcement purposes. Since this problem extends across the intelligence spectrum (not just clandestine operations) it has been treated in the *IC21 Intelligence and Law Enforcement* staff study.

investigations and violate restrictions on sharing information on such activities as grand jury proceedings.

In practical terms what this can lead to is the CS and law enforcement agencies working with the same liaison services or clandestine agents (or "informants," as they are called by law enforcement) in an uncoordinated manner and even in ignorance of each other's activities. Most of the pitfalls of this have been outlined in Finding Two. In the case of liaison, the lack of coordination may:

- confuse the liaison service as to who speaks authoritatively on which issues for the US government,
- put the liaison service in the advantageous situation of being able to play one US agency against the other,
- allow the liaison service to "triangulate" sensitive information by comparing the uncoordinated information it receives from several US agencies,
- result in the utilization of the liaison service by one agency in monitoring or even foiling a clandestine operation being run by another, or
- any combination of the above.

In the case of clandestine operations, there can be confusion on the part of the agent, reporting that will lead to "false confirmations," and unwitting compromises of security.

There currently exist a number of memoranda of understanding and informal agreements on how to deconflict these types of activities overseas, and a more comprehensive understanding, particularly applying to the FBI, has been under negotiation for over a year between the DCI and the Department of Justice. The FBI's being granted extraterritorial jurisdiction over some criminal acts outside the US in 1986 and 1988 obscured some of the demarcations between law enforcement and intelligence overseas. The need for a firmer understanding has become more immediate since 1994 with the FBI's increasing the number of Legal Attaches and liaison relationships overseas and its putting out mixed signals regarding its possible intentions to expand its running of "informants" ("agents" in intelligence parlance) overseas without the knowledge of host governments.

Two recent studies, the report of the Commission on the Roles and Capabilities of the US Intelligence Community (Aspin-Brown Commission) and the Council of Foreign Relations' report of its Independent Task Force on the *Future of US Intelligence*, have concluded, generally speaking, that the balance of law enforcement activities and intelligence equities overseas has tilted too far in the favor of the

former.[11] Moreover, it takes strong exception to the expansion of FBI unilateral clandestine operations overseas, ruling that such activities should not be allowed except in rare circumstances where they are fully coordinated with intelligence officials.

There is merit to the argument that national security interests must not be sacrificed to further law enforcement objectives. We are reluctant, however, to make any categorical statement about the universal primacy of one over the other overseas. Circumstances will be different in different cases and good judgment will need to prevail. No matter what the policy decision is, there needs to be a clear, well understood, and practical system for deconfliction in the field and at the headquarters level. For a number of reasons,[12] it is most logical to have the CS COS act as the

---

[11]In its report *Making Intelligence Smarter: The Future of US Intelligence*, the Council for Foreign Relations notes:

> As a rule of thumb, foreign policy ought to take precedence over law enforcement when it comes to overseas operations. The bulk of US intelligence efforts overseas is devoted to traditional national security concerns; as a result, law enforcement must ordinarily be a secondary concern. FBI and DEA agents operating abroad should not be allowed to act independently of either the ambassador or CIA lest pursuit of evidence or individuals for purposes of prosecution cause major foreign policy problems or complicate ongoing intelligence and diplomatic activities.

Similarly, the Aspin-Brown Commission report takes exception with the law enforcement argument that the executive branch should place law enforcement interests above other policy considerations such as the impact on foreign relations and the protection of intelligence sources and methods. To clarify policy on this matter the Commission recommends the President issue an Executive Order reaffirming transnational threats such as terrorism, narcotics trafficking, organized crime and proliferation of weapons of mass destruction are national security matters. We concur with that recommendation.

[12]First, as indicated in Finding Two, the CS, as an extension of its current role, is already the focal point for clandestine and related liaison activities for the IC. There is no such focal point within the law enforcement community: overseas the FBI, the Drug Enforcement Agency, the Customs Service, and Secret Service operate independently and do not even share a single chain of command (the first two coming under the Department of Justice and the last two coming under the Department of the Treasury). Having the CS act as the focal point for coordination avoids reopening interagency rivalries for primacy within the law enforcement community. Secondly, the scope of liaison and clandestine activities undertaken by the CS will almost always eclipse in number and magnitude those of the law enforcement agencies overseas.

focal point in identifying potential operational problems and conflicts in the field. In practical terms, this means the COS must be advised in advance of all clandestine operations and liaison initiatives in his country of responsibility. He should be empowered to make the initial determination of how to resolve these problems, with the understanding that his authority in no way extends to being able to direct law enforcement investigations or prosecutions. The COS's decision should be open to appeal to the Chief of Mission (particularly on a policy issue) or a Washington-based interagency mechanism (particularly for operational deconfliction or tradecraft judgments), as appropriate.

For example, the FBI may have a US citizen confidential informant who is in contact with a foreign relative with terrorist ties and living in the Middle East. Any effort to approach, recruit, or handle that foreign sub-source should be fully coordinated in advance with the COS, who will be able to ascertain this activity does not conflict with any other intelligence or law enforcement activity. Of equal importance, the COS, being knowledgeable of the operational and counterintelligence environment, will be able to advise and even assist the FBI to make sure the case is handled in a way that does not endanger the security of FBI officials, the US citizen, or the foreign national.

This system should also have built into it an understanding that the COS will not have unauthorized access to statutorily restricted information such as that coming from grand jury deliberations or from criminal wiretaps. Additionally, COS's must be fully trained to understand the limitations that may be placed upon their taking action on law enforcement information that could later endanger its use in criminal proceedings (e.g., "Brady" and "Jencks" concerns regarding discovery).

Also relevant to the interplay between law enforcement and intelligence overseas is the question of establishing exclusive liaison relationships, that is, having a law enforcement agency or the CS claim exclusive rights to work with a specific foreign security service. In most countries the distinction between intelligence and law enforcement is not as clear as in the US; indeed, they frequently combine the two functions in one or more security services. Accordingly, there may be compelling reasons for the CS and one or more US law enforcement agencies to have official liaison with the same service. Circumstances will dictate which US agency will have the most active liaison relationship.

It is easier to keep the CS COS informed as necessary on law enforcement activities than to have a designated law enforcement official have to keep track of the CS's activities. Finally, it is a central responsibility of the CS to monitor the local counterintelligence and operational environment overseas. That knowledge makes it the most appropriate organization to act responsibly in providing expert operational guidance, if necessary, on the conduct of activities made known to it.

Even when the overt reason for liaison is not overwhelming, it is in the US's national interest to allow the CS to maintain liaison with a foreign security service. The reasons are several. Law enforcement agencies deal with foreign entities principally in direct pursuit of specific law enforcement and prosecutorial issues. Cooperation from foreign services can be limited on occasion by the fact that law enforcement agencies, unlike the CS, cannot in most cases promise to handle the information provided under the statutes of classification that are designed to protect intelligence sources and methods. Moreover, the IC has been designed to employ collection techniques not normally available to a legal attaché or official law enforcement agency representative overseas. The information/intelligence collection technique most readily available to a law enforcement official overseas is asking questions of a foreign liaison service overtly and on the record. That option is also open to the CS, although the host country usually prefers it not be employed.

Most typically, the CS can collect intelligence from a foreign liaison counterpart at almost any level of discretion and reasonably promise him that the DCI's unique authorities to protect sources and methods can be applied to make sure the information is not used in a way that can later cause trouble for the foreign country, the foreign security service, or the liaison counterpart himself. Should those assurances be insufficient to get the foreign security service's cooperations, the CS (not being restricted by law enforcement's concern for evidentiary standards) can employ appropriate clandestine techniques. These techniques are among the most productive available to a CS. As an example, in the recent past, the DO worked successfully around and outside established channels in a foreign country to foil a terrorist attack. Hundreds of lives were probably saved. In this case, an official law enforcement to law enforcement agency relationship would probably never have led to the unravelling of the terrorist plotting.

In light of the rapid expansion of law enforcement agencies into liaison relationships abroad, the executive branch should promulgate an executive order to reflect the above finding and advise the oversight committees of Congress of any need for legislative support.

Finding #4: The Clandestine Service should service validated, high-level military requirements and have the capability in the event of deployment of US forces to surge to support low-level, tactical requirements as appropriate.

The risk/gain calculus and high standards used in vetting national requirements for clandestine collection (as outlined in Finding One) should be the same for vetting requirements in support of the military. Low-level military requirements do not usually warrant the use of clandestine collection techniques. Generally speaking, if uncovered, the level of political embarrassment for targeting a country's military secrets are likely be at least as high as for targeting its political secrets, since most governments tend

to be extraordinarily sensitive to any espionage activities directed against their militaries.

Military clandestine collectors, not being major players in the national intelligence arena and working mainly for their commanders in their service, have traditionally specialized in low-level types of operations that might be of operational utility in tactical situations. Although this was acceptable in many parts of the world and appropriate during the Cold War, the management of DHS (into which the military collectors have been consolidated) has made initial efforts at upgrading the quality of military operations without abandoning a commitment to support the tactical commander. This represented a major step forward; however, the quality of most DHS assets still appears to fall well below the appropriate threshold. This appears to result, at least in part, from an as yet incomplete understanding or acceptance within the DoD of the limitations and strengths of clandestine operations in supporting the military.

This leads to the question of how clandestine operations can satisfy the tactical needs of the commander in a deployment in a hostile environment. The proper answer, although it would probably be unsatisfying to most commanders, is that clandestine operations will in many cases be of marginal value and may be inappropriate. Clandestine HUMINT-type operations are usually poor at providing immediate, on-the-ground support, that is, telling a commander what he most wants to know: what is going on over the next sand dune or has a SCUD just been launched?

Military commanders must be better educated on what clandestine operators can and cannot realistically do for them. This will result in the better utilization of the intelligence product and wiser management of clandestine military resources. It will also mean the CS can then justifiably be held accountable for providing appropriate support to the military. For example, the CS should be able to provide the military with across-the-board support for strategic military planning against validated targets. Depending upon the adversary, its priority, and the lead time given, a successful CS should be able to provide order of battle; foreign military doctrine; readiness, industrial capacity, and logistics information; and information on the personalities at play.

The major contributions of the CS to a commander's ability to fight will have taken place months if not years prior to the firing of the first weapon. As it has over the last several decades, the CS must continue to collect technical data (e.g., manuals and research and development documentation) and exemplars of the high tech weapons and defensive systems the military will face in war. These collection activities usually take place years in advance and far away from the battlefield, but they are the crucial starting points from which are designed smart weapons and the highly sophisticated defensive and offensive weapons, such as those that were used to such great effect against Iraq's Soviet equipment during the Gulf War. Many, if not

all, of those weapons could not have been deployed with such confidence had the enemy weapons systems not been so well understood. Additionally, a military commander is justified in expecting a successful CS to have, if necessary, played a role in compromising the telecommunications and cryptographic capabilities of any potential enemy that is a validated collection target.

Having noted the limitations of clandestine operations in a battlefield situation, we note the irony that in several of the US military's most recent deployments, clandestine HUMINT-type operations provided much of the best intelligence available to the military. This was not so much due to the capabilities of clandestine collectors as it was a function of the limitations of technical collection systems in environments largely devoid of signals to collect and tanks and military vehicles to photograph.

In a low-tech military operations, clandestine HUMINT can, by default, become the most important intelligence type and for that reason it must be positioned to help the commander and protect troops. It is partially in recognition of this fact and of the difficulties in surging clandestine capabilities from zero, that we have concluded in Finding Five that the CS should opt for a global presence rather than a global reach. That is to say, the CS should maintain a small presence in most parts of the world, even when those countries do not meet the high standards of operational interests that should guide most of its activities. It is entirely too likely that the hot-spots into which US forces must be introduced will not have been predicted and will be in a country or region that would not otherwise have merited the CS's attention.

Finding #5: The Clandestine Service should opt for "global presence" rather than "global reach."

A solution to the great pressures the DO has felt since 1991 with the drawdown of resources and personnel was to move from being a service with a "global presence," that is, having a station in every country that could reasonably be of interest, to having a "global reach," that is, withdrawing from many marginal countries, but trying to maintain some sort of access and capability that can be, presumably, reconstituted and expanded if needed. Plans were made and, as has already been stated, large numbers of stations and bases have been closed since 1992. Many intelligence observers, including this Committee, thought this was a reasonable adjustment to a situation where resources in real dollars were likely to continue to decline at a steep rate for the foreseeable future. In the last year there has been a retreat in some quarters from this pessimistic resource projection; but, more importantly, many have re-thought the implications and practicality of a global reach strategy.

After much deliberation and consultation with expert practitioners of clandestine operations and intelligence managers, we believe the CS of the future must strive for

a global presence. At the least, it ought not to reduce the number of its overseas stations and bases below current levels. Two arguments are particularly strong.

First, a global presence is essential to support military requirements. Although this study strongly concludes that the CS should concentrate on the hard targets and the highest level national requirements that it uniquely satisfies, it also believes the CS of the future must accept fully the responsibility to support military operations to the degree it reasonably can. As is argued in Finding Four, the CS must accept its responsibility to support the requirements of the military not only for strategic intelligence -- something in which it can excel -- but also for appropriate tactical intelligence support in times and places of military engagement -- a responsibility that often falls to it only by default. Recent history has shown that it is increasingly difficult to know in advance where the military might be deployed and where the CS should begin building up capabilities in advance.

A second argument for a global presence is that the targets of the CS are increasingly international and transnational and a global presence is increasingly crucial to attack those targets. Terrorism, the proliferation of weapons of mass destruction, narcotics, and international organized crime are all recognized in a variety of NSC and Presidential directives as high priority requirements of the intelligence community. These are also issues on which the National Strategic Intelligence Reviews and the Comprehensive Capabilities Review have shown the policymaker is heavily reliant on HUMINT. The National HUMINT Requirements Tasking Center has, it appears correctly, given detailed and high-priority taskings to clandestine operators around the world to go against these targets. With the mobility of populations, fungibility of finances, internationalization of businesses, and advances in communications and transportation, the whole world is increasingly the playground of the targets of such operations. A weapons proliferator can set up a front company in a sleepy Central Africa capital and a terrorist cell can relocate to an obscure provincial city in South America in a matter of days or weeks. It is only by having a presence in those countries that a CS can have a stable of agents to help mount unilateral operations or be able to seek the help of a friendly liaison service. Under these circumstances, the CS cannot simply write off large parts of the globe.

Finding #6: The Clandestine Service should be under the direct control of the DCI and form a separate organization.

It is the opinion of the great majority of high-level current and former intelligence officials consulted that the Clandestine Service, whether it remains part of the Central Intelligence Agency or becomes a free-standing organization, must be under the direct and proximate control of the President's senior intelligence official, the DCI. We strongly concur.

In the first several decades of the CIA's history it was not unusual for the DCI or the Deputy Director of Central Intelligence (DDCI) to come from within the operational ranks. That not only resulted in the DCI's being strongly interested in the DO's activities, it also meant he had continuing personal insight into the DO through his personal contacts. This situation has not been the case for almost two decades, and, due to the controversy of the DO, it is unlikely to be the case again in the near future. Until recent years, though, the DCI made sure that the DDO was aware that he reported directly to him and usually viewed oversight of the DDO as being his most important responsibility along with being the President's personal intelligence advisor. It has also been one of the DCI's most demanding responsibilities. As Richard Kerr has noted from his time leading the IC and as DDCI, easily two-thirds of the issues the DCI must bring to the President and Congress have a DO angle to them. This, he says, is because of the types of information the DO collects, the problems inherent in DO operations, and the fact that the DO is the sole action arm in the Community -- "the DCI and the President depend on it not only to collect intelligence but to act on it with foreign governments, with liaison, and in other ways." The DDO's office was moved next to the DCI's in 1973 because of the need for easier interaction and more frequent personal meetings; and, as one former DDO has pointed out, it was not by accident that the DDO's office suite has since remained there -- "within shouting distance."

In recent years, however, the DCI has attempted to concentrate more on his role as leader of the IC rather than as the director of the CIA and overseer of the DO. Some have been more successful at this than others. Former Director James Woolsey, for example, started in this vein before being sucked into the Aldrich Ames vortex. The effort to increase management attention to the IC at large has inevitably led to strains on the DCI's time and to span of control problems because of the significant increase in the number of intelligence community officials reporting to him. Recent DCIs have stated that these strains are manageable by proper delegation to subordinates. The current DCI, in particular, has increased his reliance on the DDCI and the CIA's Executive Director to filter and oversee the activities of the DO. The current DCI has indicated that, rather than directly supervising the DDO, he looks to the Executive Director to be his "chief operating officer," including the day-to-day management of the DO. Additionally, he has stated that his DDCI is also responsible for overseeing the DO. As described to one journalist, the DDCI "has taken the overall supervisory role in directorate affairs, while day-to-day responsibility for decisions on personnel, operations and other issues goes to [the Executive Director]."[13] It is not clear, under this system, what the responsibilities are of the current DDO. Interestingly, none of the three -- the DDCI, the Executive Director, and the DDO -- have experience in clandestine operations.

---

[13] *Washington Post*, 27 December 1995.

Although the *IC21* studies recognize and, indeed, encourage the expansion of the DCI's Community role, it makes little sense to do that by attenuating the DCI's supervision and knowledge of the activities of a CS. Moreover, as would be the case in the military, it makes even less sense to create duplicative or even a triply redundant operational management of a CS -- particularly to the degree this process inserts inexpert judgment.

The following are a few of the arguments for the most direct and proximate DCI control possible.

1) Most of the operations of the CS are, by all accounts, the most tricky, politically sensitive, and troublesome of those in the IC and frequently require the DCI's close personal attention. The CS is the only part of the IC, indeed of the government, where hundreds of employees on a daily basis are directed to break extremely serious laws in counties around the world in the face of frequently sophisticated efforts by foreign governments to catch them. A safe estimate is that several hundred times every day (easily 100,000 times a year) DO officers engage in highly illegal activities (according to foreign law) that not only risk political embarrassment to the US but also endanger the freedom if not lives of the participating foreign nationals and, more than occasionally, of the clandestine officer himself. In other words, a typical 28 year old, GS-11 case officer has numerous opportunities every week, by poor tradecraft or inattention, to embarrass his country and President and to get agents imprisoned or executed. Considering these facts and recent history, which has shown that the DCI, whether he wants to or not, is held accountable for overseeing the CS, the DCI must work closely with the Director of the CS and hold him fully and directly responsible to him.

2) For the President and the DCI to feel confident that the benefits of having a functioning CS outweigh the risks, they must feel confident that the reporting chain is direct and personally accountable to them. Without this confidence, the CS will not be trusted and it will inevitably come under an inexpert, risk-averse bureaucratic review process, with each layer comfortable with rejecting and questioning operational opportunities but reluctant to approve them without going to the DCI anyway. The creation of a doubly or triply redundant superstructure of non-expert operational management between the Director of the CS and the DCI makes sense only if an Administration's objective is to eliminate risk even if the cost is having a CS that has little if any chance of succeeding in its most important missions. If this is the case, the IC and the taxpayer would be better off without a CS.

3) Many of the best clandestine operations develop quickly and require an oversight and approval process that, for the government, is uniquely adaptable and timely. The DCI's authorities have been crafted so that he can meet these requirements. Bureaucratic layers between the DCI and the Director of the CS are impediments to decisiveness and effective communication, particularly to the degree

that they involve the review of administrators who are not expert in understanding the opportunities and pitfalls of clandestine operations.

4) The CS is the focal point for the conduct of most US intelligence liaison activities overseas (see Finding Two) and is the arm of the government principally tasked to carry out covert actions -- that is those covert activities undertaken at the President's request in furtherance of US foreign policy. In effect, the CS, under the direction of the DCI, acts as a *de facto* clandestine or covert arm of US foreign policy. This is hardly an overstatement in several important countries where the political leaderships have chosen, for a variety of reasons, to carry out their more sensitive political discussions with the US President through intelligence rather than Department of State channels. Covert action and foreign political functions are activities very different from intelligence collection, and it makes little sense to have the IC management superstructure in the chain of command for the DCI's management of these policy related activities. Simply put, the DCI must be fully cognizant and directly in control of these activities through the individual responsible for their being carried out -- the Director of the CS.

5) As documented elsewhere in this report, the CS, despite its relatively small size in the IC, provides a disproportionate amount of intelligence of critical value to meeting national level intelligence requirements (that is those of greatest interest to the President and the NSC). When it performs well, the CS is particularly important as a source of highly sensitive information on the plans and intentions of foreign powers. In some ways the CS's importance to the policymaker is analogous to the importance of SIGINT and, most particularly, IMINT, in supporting the tactical military intelligence consumer. The placement of the CS in the IC should maximize the DCI's ability to exploit and task the clandestine system directly.[14]

6) Finally, organizational common sense dictates that if there is to be anyone responsible to the DCI for the proper administration of the CS, it should be the individual who is realistically responsible for its actions: the Director of the CS. If properly chosen and trusted by the DCI, the Director of the CS can do this job better than anyone else. If a DCI finds himself in the position of preferring to have someone other than his Director of the CS oversee the CS, he should replace the incumbent with the preferred individual, rather than create another layer of oversight by putting him above the incumbent.

Having made these arguments, there is, nonetheless, a very real requirement for an Executive Director with the authorities to manage and deconflict administrative

---

[14]Note, however, that for most tasking and requirements the CS should be dependent upon a Community-wide collection management mechanism that factors in the capabilities, costs, and relative merits of all collection techniques.

problems and act as an honest broker in resolving differences so long as the very different activities of the DO, Directorate of Intelligence (DI), Directorate of Science and Technology (DS&T) are housed together in the CIA. We have grave concerns, however, about the propriety of having the Executive Director perform the role as defined by the current DCI, that is, as the "chief operating officer" of the CIA. These concerns go beyond the issue of properly managing clandestine operations: it appears extraordinarily unwise to put one non-confirmed official in the position of managing clandestine intelligence collection, directing covert action programs, **and** supervising and influencing the production of the nation's most important all-source analytic organization. There should not be a concentration of these authorities in the hands of someone other than the DCI or a confirmed subordinate, particularly when there is no assurance that the person is a qualified intelligence professional.

Former Acting DCI, Richard Kerr, a career DI officer, proposed to the Committee that, if the current CIA and IC structure are maintained, it would make sense to have a career CS officer as the Senate-confirmed DDCI who is putting in charge of the day-to-day management of the CIA. At the least, such an arrangement would likely provide more professional oversight of clandestine operations and provide more accountability than the current confusing situation. It is less certain that this would benefit the CIA's other functions.

It is, of course, our belief that rather than modifying the *status quo,* there are real advantages for the proper management of clandestine operations (and all-source analysis) in organizationally separating the two. The current situation has resulted from the historic administrative expediency that the CIA statutorily is the only agency into which the DCI could put activities he wanted to control. There was no other managerial logic behind it, and, indeed, until recently, great care was taken to keep these two activities separate. Although there are strong arguments supporting an increase in cooperation between operations and analysis, such as currently advancing in the CIA under the banner of "DO-DI Partnership" (see Finding Eight), there is no reason the two activities must exist as elements of the same IC entity.

The creation of a unified CS, built around what is currently the DO, significantly revamped along the lines presented in this report, and under a Director fully and directly responsible to the DCI, would be in consonance with the arguments in this finding. It would also facilitate the proposal to strengthen the CIA's role, under the leadership of one of two DDCIs, as being first and foremost the nation's and President's premier all-source analytic organization (see *Intelligence Community Management* staff study).

Finding #7: The Clandestine Service (CS) should be led by career CS officers.

It makes little sense to put non-specialists in positions where the main job element is the provision of wise, expert operational direction and oversight. This is

true in choosing a general, the head of a team of surgeons, or the leader of a large legal defense team. It is also true in selecting the leadership of a CS.

As pointed out in Finding One, the most difficult operational decisions of the CS must be reviewed (and often made) by the CS leadership. This requires expert knowledge of a widely diverse set of skills and techniques unique to the CS. Additionally, managing a CS means managing a higher level of risk on a daily basis than any other job in the government. An unquestionable expertise in the business is necessary to avoid the managerial extremes of risk-avoidance and risk-blindness, the one hobbling the CS from taking those risks most important to its success, the other leading to mindless operational errors.

The current DO, for example, engages in several hundred clandestine operational acts per day -- ranging from meeting penetrations of governments to servicing clandestine technical intelligence sites. Most of these acts, if discovered, would, at the very least, involve major embarrassment to the United States. A properly run CS has to have built into it the flexibility to allow case officers to make split second decisions, but it must also, when possible, look over their shoulders, making sure they exercise proper judgment. This leads to a steeply pyramidical organizational structure. In the field, this means that operations are reviewed by one or two layers of management, and the headquarters review process may also involve several layers and offices.

The most sensitive operations may have to be reviewed all the way up the chain of command by the Director of the CS and even the DCI. A typical operational problem of this sort would be deciding whether a case officer should unload a dead drop from a extraordinarily promising but unvetted agent in a hostile country a week prior to a high-level bilateral diplomatic event. Such a problem might also involve high-level consultation outside the CS (such as with appropriate authorities in the NSC or the Department of State). First, though, it requires proper operational evaluation in the form of an operational risk/gain analysis. This requires a sophisticated understanding and appreciation of many operational factors and the tradecraft to be employed: surveillance, countersurveillance, operational testing, concealed radio communications, covers for status and action, host country counterintelligence capabilities, US operational history in the country, and a frank assessment of the operational experience of the CS officers and managers involved. Even then, making such a decision is not mechanical, a simple matter of plugging in percentages. As in playing chess or in plotting a move on a battlefield, there are too many variables, and at some point the manager must also apply the intuition and judgment that comes only from having spent years working similar problems. If the leadership of the CS is not the absolutely best available -- the wisest and most experienced -- risks are needlessly increased, opportunities are missed, and the US is not well served.

This finding, that the CS should be led by career CS officers is not the same as advocating that its whole leadership and management team should arise *sui generis.* In addition to managing operations, the director of the CS must also manage an organization. It is in this regard that the current DO has not always distinguished itself. There is a role for consultants in improving this situation and in making sure that the CS benefits from good managerial practices that are developed elsewhere. The long-term solution also involves changes to the CS personnel system, particularly as it works to develop officers who show potential for leadership. These officers should be targeted for advanced management training (assuming they do not already have significant backgrounds in the area) such as in graduate programs, and should be required to serve rotational tours outside the CS prior to advancement into the senior executive service.

Also, it is not impossible that there may be an extraordinary occasion when an individual, having developed extremely useful talents working in another intelligence or national security field, may be the best candidate to serve in a management position in the CS, perhaps even as its Director. In such a case, however, it would be essential that the Director of the CS assemble around him a management team on which he can rely for operational advice.

Finally, as a practical matter, recent history has shown that DDOs (and even DCIs) are being held responsible for operational decisions that are made during their tenures -- even at levels far below them. While this tendency may now be extreme, there is no denying, as has been strenuously argued in the Finding Six, that the country and the DCI will be best served by having a Director of the CS who can reasonably be held responsible (and accountable) for the CS's activities.

Finding #8: The Clandestine Service should be closely linked to all-source analysts on a selective basis.

The proposal to separate the CS administratively and organizationally from the DCI's all-source analytic organization is not meant to attenuate the close working relationships ("partnership") that have grown up between these two functions. An increasingly close working relationship between the clandestine collectors and all-source analysts can, in the coming years, result in significant improvements to the value of CS reporting and all-source analytic production, but only if it is carefully and thoughtfully implemented in those areas where the expertise of the relevant collection and analytic components are complementary and lead to unquestioned mutual benefit. At least from the perspective of the CS, the problems of a careful, limited partnership

should be manageable and are far outweighed by the advantages, not the least of which is the improvement of two-way communications for tasking and reporting.[15]

The 1994 announcement of partnership between the DO and DI was met with skepticism by many current and former employees of both directorates. Part of the opposition was attributable to the feeling on the part of many that too many other changes were already underway at the CIA. Another major reason was that the partnership went against a tradition of separation that, though weaker than it had been, continues. In the early years of the CIA, the division between the two functions was so sharp that one directorate's employees were not free to visit areas belonging to the other without escort. The division became somewhat less severe in the 1970s and more so in the 1980s with a program bringing DI analysts into some embassies and stations. At the headquarters level, it was the hard-fought success of the newly formed centers, particularly the Counterterrorism Center, that most accelerated the interaction of DO and DI personnel.[16] In the DO, the value of DI analysts in targeting[17] reinforced the trend: for example, Office of Weapons Technology and Proliferation personnel are integral to DO offices working proliferation issues, and DI economists sit side-by-side with DO officers to fine-tune the targeting and exploitation of foreign economic targets.

These are examples of partnership that should be replicated discretely, on a case-by-case basis where and as it makes sense. It seems likely that the area and issue expertise of all-source analysts will be of greatest benefit to the CS in its efforts to develop hard target operations and work against arcane technological and economic targets.

---

[15]For the CS, the only significant problem could be the unnecessary compromise of the principle of "need to know," that is, compartmentation of sources and methods. This would appear to be manageable if the partnership is done on a case-by-case basis. The most frequently cited problem with partnership for the analysts is in maintaining the objectivity of analysis. That is an issue beyond the purview of this study, but, again, with vigilance and attention, it would appear to be manageable.

[16]See the *IC21* study on *Intelligence Centers* for more on the benefits (and problems) involved in the development and operation of organizations merging analytic, collection, and (in many cases) policy and covert action functions.

[17]"Targeting" has become something of a term of art in clandestine operations. Success in clandestine operations is dependent on planning as well as serendipity. Targeting is meant to maximize the advantages of planning so as to be able to recruit fewer but better placed agents. All-source research is the starting point for this process, as, for example, in developing an encyclopedic database and study of a hostile nation's nuclear weapons program and personnel. The DO has found DI officers to be irreplaceable in helping with such work.

The arguments for partnership also justify closer interactions between all-source analysts and the technical collection disciplines. Nonetheless, the data (such as in the Background section of this study), showing the key role clandestine collection plays in satisfying the national level requirements that are the DI's principal focus, indicate the DI would benefit most from closer cooperation with the clandestine service. In this regard, the partnership is analogous to the closeness that has developed between SIGINT producers (via Cryptologic Support Groups) and tactical military analysts due to SIGINT's frequently predominant role in providing tactical military intelligence.

Finding #9: The Clandestine Service should manage the support mechanisms that are critical to its functioning and essential to its success and that exist exclusively to serve it.

As one former clandestine operations manager has suggested, no corporate CEO would agree to be responsible for the success or failure of his company without full control over his company's finances, travel, communications, logistics, physical plant, security, payroll and many personnel functions. Yet, that is basically the situation that exists now with the DO since the Directorate of Administration (DA) is responsible for much of the DO's administrative support and the Office of Technical Services (OTS) of the DS&T provides technical support to clandestine operations.

The CS needs, to the degree possible, to manage the administrative and technical clandestine operations support mechanisms that are critical to its smooth functioning, essential to its success, and exist exclusively to serve it.[18] In addition to making these functions more responsive to the mission, their merger in the CS may allow the service to take advantage of the increasing commonality of skills required of categories of personnel that are now spread between three different directorates -- case officers specializing in technical operations, technical operations support officers, and communications/computer systems support officers.

If the CS does assume responsibility for its technical operations support and large parts of its administrative support, it is reasonable to expect that the number of people in these activities could make up somewhere between twenty five and thirty-five percent of the service. To house, manage, and offer career development to these personnel, there would have to be a strengthened deputy to the Director of the CS responsible for all elements of support.

---

[18]Obviously, there are some administrative functions that cannot be carried out efficiently within an organization as small as the clandestine service and for which economies and efficiencies of scale can be found by keeping them part of the CIA or in the Infrastructure Support Office (see *Intelligence Community Management* staff study).

Finally, in regard to our proposal in Finding One that the CS should be kept small, the incorporation of appropriate support activities within the CS should not be considered a net augmentation of its personnel, since this change simply rationalizes the location of functions and offices that are currently outside the DO but which exist to support it.

Finding #10: The Clandestine Service requires significant changes to its personnel management and career development systems.

The outrage -- public and within the CIA -- surrounding the exposure of Aldrich Ames as a Soviet and later Russian spy who had managed to compromise many of the CIA's greatest and most carefully guarded secrets, was magnified by his having been a marginal and occasionally a problem employee whom the system had failed to remove prior to his committing acts of treachery. The Ames case, rightly or wrongly, has been the backdrop against which subsequent allegations of DO mismanagement have been viewed. Calls for radical change have come from many quarters, not the least being from the current leadership of the CIA and from former DCI Woolsey.

Most of the changes that have been made to date have involved efforts to reform defective systemic or process problems. There have been so many changes in the complementary areas of personnel management, accountability, personnel security, and counterespionage that it would take several pages to list them. Their number and the rapidity with which they have been promulgated has stretched the ability of the DO to incorporate them and make them part of the fabric of the CS. No doubt, some will turn out to be more successful than others, and it may be that some of them will result in unforeseen problems of their own. In this regard, those seeking to change the DO must be cautious not to damage those features of the "culture" that are not only good but essential to any successful CS. Sociological studies have amply proved that, just as in attempting to "improve" an ecosystem, efforts to improve or reform seemingly discrete aspects of a culture will frequently have unforeseen and unintended consequences.

For these reasons we are reluctant to recommend any but the most necessary additional changes prior to giving those already decided upon a chance to show their effect and be evaluated. There is also the knowledge that change always causes stress -- even when the intentions are welcomed -- particularly on an organization that, to succeed, is so totally dependent upon employee job satisfaction, motivation, and *esprit de corps*. Nonetheless, there remain to be made several overwhelmingly logical changes to the personnel management and career development system. Each appears to have tremendous potential to improve the CS in the long-term without running much danger of disabling the positive aspects of a successful CS "culture." Moreover, most of these proposals can be implemented incrementally and carefully monitored as they are put into effect.

The CS of the future should:

1) increase the exposure of its officers to the rest of the IC, the intelligence consumers, and Congress;

2) develop an enhanced program for recruiting new junior employees;

3) be more aggressive in identifying officers who will be CS managers and ensuring that they are qualified or will receive training qualifying them to manage;

4) reduce the rapid turnover of personnel in field and headquarters assignments; and

5) make fuller use of DCI authorities to remove marginal and unsuitable employees.

The arguments in support of these proposals are, we believe, clear and incontrovertible.

Increasing exposure to the rest of the government: An unfortunate side-effect of the uniqueness of the DO's work has been a belief that there is little advantage, individually or organizationally, in having its employees work outside of it. The DO has until very recently been content to be insular and isolated, believing its role and the value of its product were self-evident. Accordingly, DO officers felt that if the organization identified the right thing to do and simply went out and did it, the consumer would be happy and the DO would be largely immune from criticism. This is clearly no longer true, if it ever was. But it was in this way that the DO -- an organization filled with people priding themselves on being able to go into a foreign country, figure out its inner workings, and quickly learn which buttons to push -- became so willfully ignorant about how Washington, D.C. works and inept in dealing with it.

The DO's isolation has hurt it at every level. Inside the IC it has been viewed as elitist and deserving a comeuppance. For this reason there was no absence of *schadenfreude* around the IC at the DO's recent difficulties. Outside the IC, the consumers of intelligence were largely ignorant of the DO's activities and capabilities, most of them having never met a DO officer and seldom seeing a raw DO report. Further, the DO's willful ignorance of Congress was compounded by distrust and mixed feelings about oversight (which, to be fair, has been fed by some Congressional actions). An increase in the number of rotational assignments within the IC, in consumer agencies and departments, and as Congressional fellows would appear to serve well in opening up the CS to the realities of Washington, D.C. This will be impractical for most younger officers whose covert employment status must be

protected; however, it should not present insurmountable problems for most mid-level officers whose cover may have already been compromised to some degree.

The process for recruiting young, full-career employees ("career trainees" as they are called in the CIA) is in drastic need of change. In the past, the DO operated in a buyer's market when recruiting new employees. It had the luxury of being able to pick and choose among literally thousands of applicants, many with impressive qualifications, for each position it had to fill. As a result, its new recruits were usually well-educated, highly motivated, and highly qualified for the work. This situation has changed dramatically for the worse over the last two years since the Ames case. Despite the DO being significantly under its authorized personnel ceiling, it is having tremendous problems recruiting qualified new employees, although the number of applicants remains high. The current climate of public opinion being what it is, it appears unlikely that this situation will improve on its own in the next several years. This is a problem that will have disastrous effects on the CS of the future and requires immediate action. The DCI and the DDO should prepare for Congressional consideration a program of more aggressive and enhanced recruitment of career trainees. The DCI should consider reopening regional recruitment offices that were closed in the early 1990's, establishing a program of incentives for highly qualified recruits, and putting the recruitment process under the direct leadership of a highly qualified senior executive.

Identifying and training managers: The existing personnel evaluation system in the DO is arguably the best in the IC if not the government. To our knowledge, no other element of the government annually has every employee's personnel record and evaluations reviewed cover-to-cover, annotated by all members of a panel of more senior employees, and then serially rated in comparison with all peers. Moreover, the DO, like the rest of the CIA, is excellent in training its personnel in specific skills and subjects, as, for example, in languages or tradecraft skills. Yet, neither the personnel system nor training form part of a coherent program of career development for managers.

Although it is extremely likely that a good manager of clandestine operations will have started out as a good clandestine operator, it does not follow that all good clandestine operators make good managers. It is a universal observation of the experts consulted that the DO does an outstanding job of evaluating and promoting individuals who are good at what they do, but that it does not have a good system to ensure they will be good at what they will be asked to do next. To remedy this, the personnel evaluation system should be modified to identify and train (if necessary) mid-level officers entering the management ranks in the management skills necessary for them to manage well through the rest of their careers. This should include enhanced in-house training as well as a program of external training, as necessary. The CS should also revisit the possibility of setting up a non-managerial "operations track" program whereby the truly exceptional clandestine operator who cannot be or

is not interested in managing may serve out his career profitably in senior operations positions. At the very least, such a system saves the CS from having some of its management positions filled with individuals who are there for the money and recognition rather than because of their commitment and interest in the job.

Slow down the turnover of personnel: In the heyday of the 1980's when personnel resources were not under strain, the DO was able to operate under a system where there was rapid turnover of personnel at headquarters and in the field. In an organization that is smaller and more focused on fewer but better operations, continuity in leadership and operations will be increasingly important as well as efficient. To the degree that cover considerations allow, field tours should be lengthened. Headquarters assignments also should be made with an understanding that they will be filled for a **minimum** of two years at the desk and branch level and for three years at the division level, unless extraordinary circumstances demand otherwise. The current situation of most desk and branch chiefs serving a year or less while processing for field assignments or waiting for other assignments is counterproductive and feeds the perception of the field that it has no dedicated and informed personal support from headquarters. Managers at the office and division level will also manage better if they know that they will have to live with the consequences of their decisions. Making changes of this sort will fly in the face of the deeply ingrained attitude inside the DO that the field is fun and career-enhancing, while headquarters is stultifying and "dead-time." This is one of those areas of "culture" that can be changed only at great risk, since it is essential that a CS have the field as its unquestioned focus and principal interest. The CS of the future should consider, however, a system giving some sort of temporary monetary incentives (as opposed to enhanced promotion rates) to officers distinguishing themselves at headquarters, particularly if done over a two-year minimum.

Finally, the CS must make fuller use of DCI authorities and, if necessary, request new ones to enhance its ability to remove marginal and unsuitable employees. Quite simply, the stakes are too high not to do this. The CS must not only have the best system for recruiting employees, it must have the best system for removing those whom it no longer needs or wants. The current system in the DO is the most aggressive in the civilian sector of government -- actually removing a handful of employees each year; however, as the Aldrich Ames case proved, it is not vigorous enough. Moreover, there is a consensus of opinion of those consulted that marginal employees have a particularly demoralizing effect in a CS that is so greatly dependent upon its employees' having an attitude of absolute commitment to mission. Since the current DO has an effective employee evaluation system allowing it to identify marginal performers and there has been a significant increase in attention to identifying unsuitable employees, the CS should develop a program that allows it to act more systematically to remove marginal and unsuitable employees. Considering the net advantage to the CS's operations from the departure of such employees and the danger posed by their being forced out without pensions or other compensation,

the Committee should consider supporting the establishment of a program similar to the military's "selective early retirement boards" whereby a employee can be selected out and provided a package of financial benefits facilitating the transition.

Finding #11: To facilitate the highest possible standards of professional conduct, the Clandestine Service requires a system of independent and professionally competent review and adjudication regarding questions of professional judgment.

In the wake of the Ames case there has been a proliferation of systems meant to ensure the accountability of DO personnel for their professional judgments. These can involve internal DO accountability boards, CIA-wide review boards, counterintelligence reviews, and the Inspector General (IG). The processes are frequently redundant in their charters, inconsistent in the qualifications of their participants, and take upwards of a year to reach their conclusions. In an organization that demands its officers take risks, involves the use of highly specialized skills, and by definition will have numerous false starts and failures for each major success, it is essential to have a single independent, authoritative, professionally competent, and timely system of reviewing questions of professional judgment. None of the current systems meets all these criteria.

Questions of professional judgment in the military, such as accidental killings by friendly fire, running a ship aground, or crashing an airplane are examined by a board of review consisting of military officers who are technically knowledgeable and professionally experienced in the activity under review. Similarly, professional organizations exist to police the activities of various highly specialized and recognized professions, such as bar associations and medical boards. In all these cases, it is the rationale that the members of such boards have a strong interest in maintaining high professional standards and, as experts, are qualified to sit in judgment. There should be an analogous process for reviewing the professional competence and judgments of individuals in the clandestine service, excluding those issues involving possible fraud or criminal behavior that must be left to the IG. At a senior level, this process would, for example, be used to review operational decisions such as those leading to the compromise of an intelligence source due to improper handling, a COS's improper supervision of a first tour officer who as a result commits preventable tradecraft errors, or a manager who has improperly disseminated intelligence or operational information. At lower levels, it can involve any number of issues, such as the review of professionalism of employees who are chronically late, sloppy in their work, or dishonest in their dealings with their counterparts.

We envision a CS Professional Review Board (PRB) system and offer the following as a possible outline of its organization. To facilitate expertness while minimizing the likelihood of its being subject to inappropriate influence, there should be at the top of the system a Senior PRB, directed by a retired senior CS officer (civilian or military) or one serving in his last active duty assignment. Other members

of the Senior SRB should be current and/or recently retired senior CS officers having the requisite professional knowledge and experience to judge CS seniors expertly. All members of the Senior SRB including its director should be nominated by the Director of the CS and approved by the DCI. The Senior PRB will be responsible for reviewing all questions of professional judgment and competence involving senior CS officers and will, in any specific case, include only those members having no personal interest or prejudice concerning the matter or individual in question.[19]

The Senior PRB should also oversee the activities of PRBs reviewing activities at lower levels in the CS. These could be similar to the newly created DO Divisional Accountability Boards with the limitation that their purview should extend only to those cases not involving senior CS officers. A member of the Senior SRB should be an *ex officio* member of all PRB reviews, and the Senior PRB should be authorized to examine all PRB decisions for fairness, accuracy, and completeness. The Senior and divisional PRBs should be given unimpeded and complete access to all information necessary to carry out their duties. The process should be transparent to the IG, and their findings should be shared with the IG to ensure he is aware of any information developed that might bring the issue at hand under the IG's purview.[20] PRBs should also have at their disposal the investigative resources of the DCI's Counterintelligence Center,[21] where the Senior PRB should also be housed with a minimal full-time administrative staff.

FINDING #12: Clandestine Operations and the Military: Civilian and military clandestine collection operations should be jointly managed within a unified Clandestine Service under the policy and operational guidance of the DCI and with an active duty two-star military intelligence officer as a Deputy Director of the Clandestine Service responsible for ensuring appropriate support to the military. Key to the success of the joint service will be the development within the military of a clandestine collection cadre that can function within the unified clandestine service at the same professional level as the civilian cadre.

---

[19]In cases where the Director of the CS's professional judgment may be an issue, the DCI should have the option of himself choosing the membership of a Special PRB.

[20]In DoD, the investigations and deliberations of panels are not transparent to the IG. Indeed, there is no regular sharing of findings with the IG, except when the panel believes it has uncovered possibly fraudulent or criminal activity.

[21]The *IC21 Intelligence Centers* staff study, proposes that this Center remain within the CS performing the same functions it does at present.

Background and Overview

Although the CS's strengths are predominantly in the area of fulfilling national level collection requirements, we strongly believes the CS must have support to the military as one of its key roles. Clandestine capabilities in support of the military are currently disjointed, poorly managed, and even dysfunctional. The "Aspin-Brown" Commission, citing criticisms of the military's poor management and minimal success in running clandestine operations, has recommended that DoD should get out of the business of clandestinely recruiting human sources and that it should become the exclusive province of the CIA, "utilizing military personnel on detail from DoD, as necessary." We concur with this judgment, placing all clandestine collection capabilities in the CS, but prefer a more active role for the military personnel assigned to the CS than the Commission language implies.

The military services' record of running clandestine operations has been mediocre. The newly created Defense HUMINT Service (DHS) into which the individual services' clandestine operations have been consolidated, has remedied some problems but exacerbated others. Specifically, the creation of DHS has alienated what little support there was for clandestine operations in the services and with the CINCs while, at the same time, bringing these operations more closely under the inexpert and cumbersome oversight processes of the Office of the Secretary of Defense (OSD).

The situation at the CIA also is of concern. The CIA/DO's commitment to support the military has been inconsistent since the end of the Vietnam War. The improvements made in the wake of the Gulf War, although positive, are not deeply rooted, and the DO has been reluctant to make further commitments to provide direct support to the military since that might put it in bureaucratic conflict or competition with DHS. At the same time the DDO, as the National HUMINT Collection Manager, has not provided DHS with the strong operational guidance it needs to develop a coherent long-term strategy for deployment of its operational resources. In short, radical changes are required for the CS of the future if it is ever adequately to meet the challenge of supporting the military.

To facilitate *IC21* examination of this issue, the Committee requested, in the classified annex to the FY 1996 authorization, that the DDO (in his role as HUMINT collection manager), form a joint task force of high-level clandestine operations officers from the DO and DHS to look into the issue of improving and integrating the two services' support to the military. That report, dated November 13, 1995 and attached as an appendix to the classified version of this study, gives an excellent analysis of many of the current structural and managerial problems and provides some proposed solutions. We are, in general, strongly supportive of the task force's findings and believe that, if fully adopted, they would result in numerous incremental improvements that would, in aggregate, significantly improve some aspects of the existing situation. Yet, the changes it proposes leave fundamental problems untouched, probably as

being politically and organizationally "too hard." It is in no way a criticism of the study to acknowledge that it had to restrict its suggestions to those that would not challenge the charters of the DO and DHS, the cumbersome military personnel system, or OSD prerogatives in overseeing one of its own agency's activities. However, in the context of the *IC21* study's look to the future, we are not bound by these restrictions; indeed, its purpose is to look beyond the current realities and address fundamental problems that go to the very core questions of organization, roles, and missions. The potential gain from rethinking the whole organization of clandestine collection for the military warrants the difficulties of taking on existing parochialisms and mindsets.

We strongly believe there must be a single US CS into which are integrated civilian and military clandestine collection. As discussed in Finding Six, this new organization, the CS, should exist as a discrete entity in the IC and come under the DCI's direct control. It will devote the great majority of its resources towards the national collection requirements that clandestine operations are uniquely suited to satisfy. It would also, however, have folded into it a permanent requirement to be more responsive to the military in the formulation of national clandestine collection plans and ensure greater support to the military commander as needed when US forces are deployed overseas. Its military cadre should be of a size necessary to meet the requirement for clandestine collectors with the cover and expertise of active duty military personnel -- perhaps ten to twenty percent.

The creation of this new joint organization would involve tremendous changes and may meet strong institutional resistance, particularly within the Department of Defense. If successfully implemented, however, it would result in the rationalization and enhanced management of all national clandestine collection resources, tremendous synergy from the melding of talents and varieties of access, economies of scale, and greatly improved collection for all consumers -- national and tactical military.

In the following, we will discuss some of the critical issues that must be addressed to bring the military into a joint CS: building a cadre of military clandestine collectors, managing support to the military, and the proper oversight of military clandestine operations.

Personnel

On the civilian side -- that is, within what is currently the DO -- many of the most serious challenges to creating a joint CS have been addressed by other findings in this study. Finding Four argues that the CS must better service-validated, high-level military requirements and have the capability to support low-level, tactical requirements as appropriate. This must become an intrinsic part of every aspect of the CS's strategic planning. Finding Five outlines the judgment that the CS must have a global presence, particularly because military contingency collection requirements

are so difficult to predict in advance. Military clandestine collectors could be instrumental in filling the requirement to staff these "military contingency" locations.

To the degree that cover concerns can be met, career military and civilian members of a joint CS should be able to serve interchangeably in all clandestine service positions in the field and at headquarters, and assignments should be based solely on qualifications and relevant operational experience. These would be deep "cultural" changes for a civilian clandestine collection community that has grown accustomed to viewing most uniformed clandestine operators as being a grab-bag of officers of varying levels of talent, with limited training, and even more limited experience.

The military services must meet the challenge of helping produce this cadre of talented, well trained, and experienced uniformed clandestine collectors. This will require some strong direction from the very top of DoD, in OSD and at the Joint Chiefs level. Without that sort of leadership, history shows us that the services are likely to pay only lip service (if that) to supporting the creation of a unified CS. In the best of times the services have not seen fit to recognize clandestine operations as a *bona fide* military career specialization and there is unanimity of opinion that there have been definite career disincentives to working in that area. Now the services and the CINCs, having lost "ownership" of clandestine resources with the creation of DHS, are even less enthusiastic. Several individuals have advised that the military services have informally counselled their best HUMINT officers that their careers will be jeopardized by accepting assignments in DHS. Without commitment from the top, there will be a continuation if not a worsening of the services' current lackluster support for the development of a program to select, train, and nurture career clandestine collectors.

There are numerous ideas on how to build a strong military clandestine collection cadre within a unified CS. The following is offered as an example that may have merit. First, the services must work with the CS to recruit highly qualified individuals from those on active duty, in ROTC programs, and in the service academies. The selectivity of the military cadre must be equal to that of the civilian. The services must then work with the CS to develop covers, training programs and career tracks that will give these recruits the military experience necessary to satisfy military requirements expertly as well as a high level of competence in clandestine operations.

Management of Clandestine Support to the Military

The designation of a Deputy Director of the Clandestine Service for Military Intelligence (DDCS/MI) at the two-star rank may be essential to the success of a unified CS. The position will expand upon the position of Assistant Deputy Director of Operations for Military Affairs (ADDO/MA) created in the aftermath of the Gulf War. The ADDO/MA, with the strong support of the DDO, did an outstanding job of

increasing the CIA/DO's responsiveness to military intelligence consumers. Moreover, this success (as is not always the case) was widely acknowledged, particularly at the regional unified commands.[22]

An important element of the DDCS/MI's duties should be his having direct control of CS support cells that are embedded in the regional commands and other important DoD entities. These cells should operate much like the National Security Agency's "Cryptologic Support Groups" and act as the Community's single focal point for the development and implementation of the clandestine operations element of intelligence support doctrine.

Oversight of Clandestine Operations Involving Military Personnel

For this or any other military clandestine operations activity to succeed it must be removed from the direct regular operational oversight of OSD. The OSD guidelines and procedures developed in 1994 and 1995, and under which DHS now operates, have shown themselves to be cumbersome, time-consuming and (some would argue) subject to political manipulation.

Findings Six and Seven of this study discuss at great length the reasons clandestine operations require nimble, informed operational oversight. These reasons apply equally to operations undertaken by civilian and military operators. The current system in place in OSD ensures decisions on fast-breaking sensitive operations are made only after months of "staffing" and at a bureaucratic level far removed from anyone having direct knowledge of the relevant facts. It is a formula for guaranteeing a risk-adverse, bureaucratic, and mediocre CS. As proposed under this finding, all clandestine operations carried out by the unified CS would come under the operational and policy oversight procedures set up by the DCI, using his authorities. The DDCS/MI will be positioned in the CS to ensure that the operations do not run afoul DoD regulations and guidelines and to facilitate any necessary deconfliction. Also, there should be built into the system a procedure whereby appropriate DoD officials are advised and consulted regarding particularly sensitive operations involving uniformed personnel.

---

[22]It is unfortunate that the ADDO/MA position and office were abolished in 1995 and the responsibilities divided between several new positions as part of the DO restructuring. Characteristically, this was done without consultation with the military consumers who, so far as we have been able to learn, had been extremely pleased with support from the ADDO/MA and his office.

Conclusion

Even if it is decided that, for bureaucratic or organizational reasons, this finding is too revolutionary and difficult to enact, we strongly recommend that DHS's give up its sideline of clandestine operations and concentrate its efforts on its larger, more productive and cost effective overt collection mission. It is our belief that DHS' clandestine mission is unlikely ever to rise above built-in limitations and justify the cost and risks involved. Even if the military does not opt to participate fully in a joint CS, we would like to see DoD detail to the CS a small number of select officers. The potential advantages of a small program of this sort should be sufficiently apparent to DoD to warrant its approval, even if DoD is unwilling to participate in a full-fledged joint CS.

INTELLIGENCE COMMUNITY "SURGE" CAPABILITY

Executive Summary

The Intelligence Community (IC) in the 21st Century will face a world that presents different, more diverse national security challenges than those presented during the Cold War. At the same time, many of the issues and intelligence problems that were spawned from the Cold War remain, and the IC is expected to address the new and the old challenges with resources that have decreased significantly since the end of the Cold War. Ambassador Robert Kimmitt, former Under Secretary of State for Political Affairs, in testimony to the Committee, suggested that whether the IC remains relevant and effective may well depend on its ability to be an "inch deep" in everything, with the ability to have a "miles worth of depth" on a specific subject at a moments notice. Creating such a responsive IC will require increased internal operating efficiencies; a more collective, corporate approach toward utilization of resources; and structured programs that provide continuous resource augmentation and "surge" capability.

This "surge" capability needs to be flexible, dynamic and well-planned -- one that can be relied upon both day-to-day and during crises. "Surge" can be defined very broadly, including the ability to: move resources quickly to address immediate, usually *ad hoc*, needs; augment existing resources from outside the IC; and, improve responsiveness of resources by building in more flexible options for collection and analysis. Taken together, these capabilities should provide for the development and maintenance of some level of knowledge on all countries/issues -- an intelligence "base." This "base" of knowledge is critical for providing predictive, timely and relevant analytical support to policy makers, particularly prior to and during fast-breaking crisis situations. As Representative Dicks, the Committee's Ranking Minority Member, has stated, "intelligence must provide early warning of potential crises or assist in developing sound policy responses to national security threats."

In order to provide crisis warning and aid in policy formulation, the IC's ability to maintain an intelligence "base" cannot be sacrificed in order to focus entirely on other, more immediate concerns. Maintaining its "base" will be an ongoing challenge for the IC as it faces increasingly diverse intelligence requirements based on policy makers' immediate national security concerns and a voracious military customer that sees intelligence becoming even a more integral part of the modern battlefield.

To address the need for "surge" capability, we make the following recommendations:

- The development of more flexible collection capabilities that not only include moving to smaller satellites but also to developing and incorporating "tactical" satellites and other assets, such as Unmanned Aerial Vehicles, that would allow for a "surge" in collection capability for a specific crisis. Such capabilities should respond to both tactical and national requirements.

- Provide the DCI with the ability to transfer personnel and resources rapidly throughout the IC, and to have the capability to bring "surge" resources into the IC from other areas. The DCI must have the ability to establish IC Centers and Task Forces quickly and with full Community participation.

- An IC-wide Civilian Reserve Program should be established that can be utilized to provide both "trends" and "warning" information and can be used to "surge," thus augmenting existing IC assets, especially during crisis.

- Better utilization of existing military intelligence reserve units is also required. This should include more focused, corporate management and tasking of these assets during peacetime, with oversight responsibilities by the Director of Military Intelligence.

INTELLIGENCE COMMUNITY "SURGE" CAPABILITY

Scope

Throughout the review of the Intelligence Community (IC) during the 104th Congress, a wide spectrum of intelligence producers and consumers have consistently voiced concerns about the need for a change in the skills mix of the analytical population and the need for additional analysts. Those in the intelligence collection areas would argue that, based on problems identified in DESERT STORM and on the potential demands for intelligence support to military operations (SMO), a similar problem exists for collection assets. Yet, the IC is continuing to undertake significant, Congressionally-directed reductions in personnel as a response to the end of the Cold War. Indeed, given the amount of intelligence resources devoted to the Soviet Union, it seemed logical that without this threat the IC would only need a fraction of the resources it had during the Cold War.

Most would argue that the "downsizing" was necessary and will be good for the IC in the long run. Many who have to deal with the IC, especially from the "outside," would agree that the bureaucracy tends to impede the efficiency of intelligence operations. Under the current system, evaluations of the success of national-level collection is primarily left up to those who operate the collectors and base their judgements on the amount of information collected by a particular system and in what time period the information was collected, rather than on whether the intelligence questions were answered.

Since the end of the Cold War, the IC has had to deal with increasingly diverse policy maker requirements. At the same time, its resources have shrunk considerably. Unfortunately for the IC, it cannot take the position that it "can't do everything," because policy makers simply expect the IC to be able to respond to a variety of requirements regardless of resource constraints. The dilemma facing the IC was summed up well during an *IC21* hearing by Ambassador Robert Kimmitt, former Under Secretary of State for Political Affairs. Ambassador Kimmitt testified that the challenge for the IC in the future is that it has to be an "inch deep" in a thousand things all the time while also being able, when a particular issue arises, to have a "mile's worth of depth" on that subject. If true, and apparently borne out since 1989, the ability to build extensive data bases and conduct more "predictive" and "warning" analysis for all areas of the world will be key to IC effectiveness in the future, as will be the ability to redirect assets -- collectors and analysts -- very quickly to new and in some cases, unanticipated problem areas.

A principal reason for this study, then, is to examine the dichotomy between growing requirements (i.e., increasing requests for IC involvement in military operations and in the policy process) and the reduction of IC resources. If the IC is to continue to be relevant, its ability to "surge" resources to meet demands must be improved. Such "surge" capability can be defined very broadly, including the ability to: move resources quickly to address immediate, usually *ad hoc*, needs; augment existing resources from outside the IC; and, improve responsiveness of resources by building in more flexible options for collection. As important, improving the efficiency of the existing IC by restructuring or reorganizing resources can also have a significant effect on the ability of the IC to meet future challenges. The importance of having or developing "surge" capabilities is quite clear -- the IC will likely never be as large as it was in the 1980s even though the demands on the IC will continue to grow.

Approach

The "Surge" Study Team approached this study by looking at the breadth that the IC must acquire in order to be effective in the future. The Team conducted panels and interviews that included individuals both inside and outside of the IC. Several questions were asked of those interviewed, including:

- What are the core capabilities that are "generic" to collection, analysis and dissemination resources that would form a "21st Century baseline" for the IC?

- What are ways that the IC could "surge" to meet unexpected challenges?

- Does the DCI have the necessary authorities to quickly move resources -- collectors, analysts and funds -- within the IC to fully address *ad hoc* "surge" requirements. What administrative hurdles must be addressed in order to achieve "portability" of intelligence resources (i.e., resources that can be moved and utilized throughout the IC)?

- Because of developments in areas such as information technologies and communications, can some "portability" be achieved without physically moving resources? Should the IC consider "specialty nodes" whose expertise can be "tapped" when needed for certain specialties? Does this benefit either tactical or strategic analysis?

- In the present day IC, managers tend to feel threatened by the loss of personnel dedicated exclusively to their workload. How can supervisory fiefdoms be made more "Community" in outlook? How can contributions to "Community" needs become a positive factor in the overall assessment of employee and unit performance?

- What type of substantive "surge" capability should exist?

- How does the IC "tap" into resources within academia or industry? Is this sufficient? Is a Civilian Intelligence Reserve Program a viable option?

- Should portions of the current or future IC function be privatized in order to utilize scarce resources in other areas? What areas might be subject to privatization?

- What effect, if any, does DoD's focus on being able to respond to two Major Regional Contingencies (MRCs) have on how the IC should be structured, particularly in terms of its ability to "surge?"

In order to assess likely "surge" requirements for the future, the study also examined recent events where some "surge" capability was required for support to "other military operations" (OMO).

Meeting Challenges Today

Showing responsiveness to civilian and defense policy makers' concerns is clearly a desire of any intelligence organization. As a result, today's IC tends to respond (either in actions or in budgetary requests) by lurching to the *issue du jour* or crisis of the moment. This suggests that, in the future, without a dedicated effort to develop and maintain an intelligence "base," a growing imbalance in knowledge can develop in lower-priority areas. Consequently, without a dedicated effort to develop and maintain some sort of "surge" capability, the IC may have difficulty meeting near-term challenges and may not be able to meet military and policy maker needs in the future. We have already seen some evidence to justify this concern. For example, the IC has responded to Presidential Decision Directive-35 (PDD-35), by focusing resources on the highest priority issues at the expense of maintaining basic coverage on "lower" tier issues. PDD-35 is an important document in that it presents the Administration's highest national security policy priorities, thereby providing the IC guidance for resource allocations. In a recent IC study of the capabilities of existing resources to meet PDD-35 requirements, the Deputy Director of Central Intelligence directed that the study, "Review the Community's core capabilities mapped against the highest policy priorities in order to determine the most cost effective allocation of

resources." Although this effort is laudable, the Study Team is concerned that in the rush to fulfill top PDD-35 requirements, the IC may be creating intelligence gaps in other areas.

Indeed, the IC is responding to PDD-35 in a predictable fashion eager to show the Administration that it is responsive to these priorities. However, the IC over-emphasis on the "top-Tier" issues could be harmful to the IC's future capabilities. For example, when considering that four of the last five deployments of U.S. military forces for OMO were to countries/regions that were, at best, "lower-Tier," the ability of the IC to provide intelligence support to OMO in the future is called into question if the preponderance of resources is almost entirely on "top-Tier" issues.

Likewise, emphasis on "higher-Tier" issues focuses attention (and resources) to areas that already have been identified as being national security "threats." But what about those "threats" and situations that have not yet been identified? As Assistant Secretary of State Toby Gati recently told the Senate Select Committee on Intelligence, "Intelligence can play a vital role in identifying opportunities for diplomatic intervention and provide critical support to our Nation's policy makers as they seek to resolve problems before they endanger U.S. citizens, soldiers or interests, and as they negotiate solutions to festering problems. This is the essence of 'intelligence in support of diplomacy,' an often ignored but vital component of our national security." Again, issues such as those described by Assistant Secretary Gati are likely not to be at the highest "tier" on a day-to-day basis.

The PDD-35 priority structure has had an effect on intelligence requirements for "lower-Tier" countries. For example, SMO, which is PDD-35's top national intelligence priority, is a top collection priority for many "lower-Tier" countries. SMO-related intelligence requirements would include information on the size, capabilities and locations of a country's military forces, and physical details about a country's topography. This information is deemed necessary based on the possibility that U.S. forces may have to operate in a particular country in the future. Other "non-military" requirements for these "lower-Tier" countries, however, such as a country's political climate, economic structure and internal stability, are of much lower priority or not reflected as having any priority. Moreover, the growing number of SMO requirements threaten to consume resources that could be used to address non-military requirements. As a result, the Community may spend more time gathering intelligence for potential SMO than for monitoring other developments that might aid in supporting diplomatic efforts to prevent a situation where deployment of forces would be necessary. Ironically, several of the Commanders-in-Chief (CINCs), expressed the desire to have the type of non-military information that was traditionally important only to civilian policy makers. Changes in world events and in the demands being placed on the military for OMO are making the need for this type of information as important

as the need for the more traditional military-related information -- a situation that many of the CINCs believe will continue to increase in importance.

Yet another concern regarding reliance on the "tier" structure is the assumption by many that other government resources, especially diplomatic resources, will supply the necessary intelligence for the "lower-tier" countries. Unfortunately, U.S. diplomatic resources are undergoing the same downsizing and concurrent reduction in diplomatic reporting capabilities as is the IC, and in the same areas. (See the *Intelligence Requirements Process* staff study for additional information regarding PDD-35 and the Tier structure.)

As stated above, the IC recently conducted an assessment of the effectiveness of its current capabilities when mapped against the Administration's highest policy priorities. This study proved interesting to the Study Team in terms of how the IC can address today's issues, and whether it is suited to meet the challenges of the future effectively. We believe that this study, which was well done, suggests that even with recent resource reductions, the IC can respond to many tasks levied by the policy makers. The study also highlights, however, several points that should be disconcerting to those concerned about the IC's future ability to address national security challenges. An important area is what the parameters do not include, which tends to portray a utopian national security "environment."

- The fact that the study did not account for tasking conflicts bases the analysis on a premise that there is only one primary issue of national security at a time, or that multiple areas of focus are geographically separated so that there is no competition for resources. An environment in which there is only one high-level policy concern at a time does not exist today and seems highly unlikely in the future, given the track record that the world has witnessed since the end of the Cold War.

- By not including warfighting needs, the assessment side-steps what is one of the major priorities of current IC leadership: SMO. The amount of resources used in DESERT STORM were significant; the vast majority of intelligence effort, in fact, was redirected to that region. The tendency of the IC to focus on the crisis of the moment, though understandable, can diminish effort in other areas.

- The parameters state that the study may not represent "current daily performance." Thus, the ability of the IC to "surge" to meet requirements was of extreme importance. A logical extension of this is that, on any given day, a question may be difficult to respond to without "surging" resources.

- Finally, by not including a survey of customer satisfaction, the IC has deliberately studied a point in time, somewhat ignoring the likelihood that requirements will grow. So, legitimately, this study reflects where we are today, not how the IC is prepared for the future.

As a result, the overall effectiveness of the IC in terms of meeting future needs and challenges appears somewhat fragile, thus warranting the development of a stable, reliable, dynamic "surge" capability for crisis and non-crisis periods.

The IC has begun to realize that there is a flaw in the PDD-35 philosophy, or certainly in how the Community is responding. A Strategic Resources Planning Task Force has been established and is working to address the philosophic and resource shortfalls that PDD-35 is creating.

"Surge" in Today's IC

There are many recent examples where a "surge" capability has been used by the IC. Clearly, the military intelligence organizations have practical experience at "surging" resources between theaters to support specific crisis situations. There are also other, more technical examples where "surge" has been successful. The development and use in Bosnia of Unmanned Aerial Vehicles (UAVs) and the emergence of IC Centers are both variations on the "surge" theme. But today, the concept of "surge" tends to be viewed more as an emergency stop-gap measure for crises in places like Rwanda and Somalia, than as a well-planned capability to be consistently relied upon. Given the frequency in which the U.S. is engaging, and likely will continue to engage in OMO, a continued reliance on *ad hoc* measures seems inadequate.

The concept of "surge" has applications in the areas of collection, exploitation and analysis and production.

Collection

U.S. involvement in Bosnia and other places, has indicated that "national" collection assets that were the bedrock of our collection efforts against the Soviet Union may not readily answer the needs of the future.

In Bosnia, the IC has "surged" to meet some additional requirements by employing UAVs. These vehicles have proven to be flexible in terms of tasking and in operating under difficult weather and terrain conditions. Although not a replacement for "national" assets in terms of the overall collection requirements, UAVs are proving to be viable "surge" assets, especially for tactical situations. The use of

UAVs on a high priority national issue like Bosnia, however, has raised complications about handling ostensibly tactical collection and keeping national-level leaders informed. As information technologies and "surge" capabilities continue to evolve, the policy issue of theater-to-national dissemination of intelligence will become extremely important to the effectiveness of the IC, especially in the all-source area.

Tasking/Exploitation

Various examples of surge capability are available in this area. One example is the deployment of National Intelligence Support Teams (NIST) to "forward" areas in order to augment military capabilities, as well as to assist theater commanders in understanding what "national" systems can provide and how they can be tasked. The response to NIST deployments has been overwhelmingly positive. That NIST in essence provides a type of synergistic, horizontal approach to collection, suggests that such an approach could be beneficial on a larger, Community scale.

Analysis and Production

Providing "surge" capability in the area of analysis is currently not as dynamic a process as it is in other areas. The National Intelligence Council (NIC) has made an effort to hire individuals working outside of the IC as National Intelligence Officers (NIOs). Not only can these NIOs bring differing perspectives to an area of concern, they can also utilize their contacts, usually in academia, to "tap" into noted expert resources that the IC does not have internally. In many cases, it can be useful for the IC to have access to noted non-IC experts from academia and industry because of their access to various forums and other experts who would not ordinarily avail themselves to government employees. Another example of "surge" capability can be found in a small program within the CIA called "when actually employed" or WAE. WAE, which is more of an employment status than a program, is utilized by individuals who are former employees or spouses of Agency employees. WAEs are asked to maintain a level of expertise in a specific area, sometimes by utilizing open source research, so that if a crisis develops, he or she can bring his or her expertise to CIA Headquarters to augment an office or task force throughout the crisis period.

To a point, current IC Centers represent a longer-term "surge" capability in which the IC has brought together its assets to focus on a specific issue or area. It is possible that such a structure may prove the most effective mechanism for concentrating IC efforts against specific issues. See the separate staff study on *Intelligence Centers* for more details.

Clearly another area of "surge" is found within DoD in the military services' reserve programs. This structured program has provided invaluable force augmentation to active duty units and, although the results vary with various units and areas of expertise, the program may serve as a model for developing similar capabilities in the area of civilian intelligence. Unfortunately, military intelligence reserve units continue to be thought of in terms of "mobilization" resources only, without much consideration or desire to more actively engage these resources in day-to-day activities.

There are signs of changing attitudes, however, that could have significant pay-off for the military and the IC in the future, although these efforts are the exception rather than the rule. One example is found at the Joint Intelligence Center in the Pacific Command (JICPAC). In this case, the JICPAC J-2 has involved military reserve resources within his theater to assist in JICPAC's delegated production responsibilities. This effort has provided the J-2 with additional resources to combat shortfalls, and has added theater-specific expertise to the DoD production operation -- expertise that is likely not found readily at DIA or CIA. Another example is the use of the Joint Intelligence Reserve Unit to support operations in the National Military Joint Intelligence Center (NMJIC) at the Pentagon. This reserve unit takes over the weekend operations of the NMJIC and has the capability to augment the NMJIC during crisis periods. Such activity not only greatly benefits the active duty military by relieving them of staffing responsibilities on weekends, it also greatly enhances the military's augmentation capabilities by having individuals who are trained, up to date substantively, and can be relied upon at a moment's notice.

Advances in information technologies and communications capabilities are forecasting an era by which "surge" capability will also be enhanced through collaborative analytical efforts within existing IC assets. Efforts such as INTELINK, that provides more advanced, multi-media dissemination capabilities for the recipient to utilize in his or her timeframe, go a long way in recognizing what technology is bringing to the intelligence analyst.

Additional efforts are underway throughout the Community to construct systems tailored to the analyst's or recipient's environment. A "white board" capability on INTELINK will undoubtedly prove useful in asking questions and working through answers in a "virtual" environment. The Study Team found these efforts most encouraging, although there are some reservations regarding infrastructure standards and information/production management. Standards are extremely important in a "virtual analytic environment," and they need to be set and enforced at a Community level to be successful. (See the *Intelligence Community Management* study regarding an Infrastructure Support Office.) Management of information is a more difficult issue. As the Committee stated in the FY96 Authorization Bill, there is

concern about competition developing within the Community in terms of publication of products. It would indeed be unfortunate and, ultimately damaging for the IC should a "competition for market share" develop. This is one reason why the DDCI heading the CIA must have management authorities for all-source analysis and production, with close cooperation of the Director of Military Intelligence (DMI), to assure "lanes of the road" are being heeded.

The Study Team believes that the direction taken by DIA in developing a Joint Intelligence Virtual Architecture (JIVA) is correct in terms of standards and development of a "virtual analytic environment." The Team believes that this effort should be not only strongly supported but also used as a basis for a Community-wide program.

Surge Capabilities for the Future: Conclusions and Recommendations

Unpredictability is one of the facts of life affecting all intelligence systems. No requirements process will be able to predict all of the issues that are likely to be of paramount interest to policy makers in the course of any given year. Indeed, flexibility of all resources -- technical and personnel -- are necessary in order to respond quickly to new events. During an *IC21* hearing, Representative Dicks, the Committee's Ranking Minority Member, explained the uncertainty of future intelligence challenges by stating that: intelligence must provide early warning of potential crises or assist in developing sound policy responses to national security threats; it may not be as important for the IC to be able to identify, with specificity, future intelligence targets as it is for the IC to ensure that it has the flexibility necessary to respond quickly and competently to those targets, whatever they may be; and, now and in the future, events will unfold quickly and unpredictably, and the IC will have to figure out how it can make information more readily available to those who can help U.S. interests, while still protecting sources and methods.

The problem of requirements and resources has been made increasingly difficult in the post-Cold War world. The end of the Cold War not only removed the single overwhelming focus of the IC, but also contributed to a breakdown of international order in specific regions, which contributed to the growth of ethnic warfare and exacerbated a number of transnational issues. A rapid succession of disparate but not wholly dissimilar issues -- Somalia, Haiti, Rwanda -- have put added stress on the IC. Before these crises arose, most of these were areas of little, if any, interest to policy makers and, thus, to the IC. Consequently, the ability of the IC to "surge" resources -- *i.e.*, to focus collection and analysis, and sometimes operational capabilities -- on these suddenly important areas, is of increasing importance.

As stated earlier, one of the witnesses at an *IC21* hearing, Ambassador Robert Kimmitt, put it succinctly when he said that IC coverage must be an "inch deep" and a "mile wide," with the ability to go a "mile deep" on any given issue.

- **FINDING: The IC must be able to surge. As Ambassador Robert Kimmitt put it succinctly, IC coverage must be an "inch deep" and a "mile wide," with the ability to go a "mile deep" on any given issue.**

As long as we are a nation with global interests and global commitments, we will need some level of global knowledge -- an intelligence "base." However, in a nation as rich as the United States is in information and experts, it is not necessary that this knowledge base be contained only in the IC.

- **FINDING: The IC will be required to maintain some level of knowledge on all nations/issues at some level of detail -- an intelligence base. The capability to support this base or to "go a mile deep" need not be self-contained within the IC.**

The ability to surge means, in effect, the ability to marshal and move resources flexibly and quickly, without undue concerns about who "owns" the assets. As the IC moves to a more corporate approach, all components and all personnel must focus on performing the tasks at hand and not battle over which component gets the most resources or credit. Internecine competition undercuts efforts to meet intelligence needs. The ability to surge also requires planning *in advance* of the need.

- **FINDING: The ability to meet future challenges effectively will require: increased internal operating efficiencies; a more collective, corporate approach toward utilization of resources; and structured programs that provide continuous force augmentation and "surge" capability.**

If done correctly, a surge capability should serve both the day-to-day needs of the IC, as resources are constantly readjusted to meet international conditions and shifts in policy maker needs, and allow for making larger reallocations of resources during crises.

- **FINDING: A flexible, dynamic and well-planned surge capability must be developed that can be relied upon both day-to-day and during crises.**

Reorganization of Existing Collection Resources

Some specific changes should be adopted to increase efficiency for the IC and the customer in the area of collection. Fully adopting a more synergistic approach to collection resources in terms of requirements and tasking management as well as operations will likely improve IC capabilities to solve the diverse intelligence problems of the future. For example, consideration should be given to a single "Technical Collection Agency" that consolidates IMINT, SIGINT and MASINT resources in order to realize the substantive advantages of synergistic collection in solving intelligence issues. Such an organization should eliminate the administrative and substantive barriers of existing "stovepipes," allow for easier, more effective tasking mechanisms for the customer, reduce some of the redundancy in collection between "INTs" and allow for better planning mechanisms for future systems by placing emphasis on intelligence needs, not the ability of program managers to "sell" their programs.

Developing the capability to "surge" national collection assets should go beyond the requirements and tasking mechanism. Further development of other collection assets for use in augmenting national resources, such as UAVs, will prove to be useful in closing some collection gaps efficiently and effectively, but only if considered as part of an overall architecture of collection resources. To address these areas further, consideration of a more consolidated IC approach for development of collectors such as UAVs is warranted. Such an approach should not overlook the uses of these collectors for other IC requirements not necessarily associated with the military.

As noted in the *Collection Synergy* study, the ability to do "all source" collection and analysis is a key to U.S. intelligence philosophy. There is an ongoing debate within the technical collection community and the Congress about future directions for satellites, revolving around the issues of size, capabilities and numbers. Although the smaller satellites that some are advocating -- including the House and Senate Intelligence Committees on an exploratory basis -- might not match the current large satellites in terms of the number of tasks that could be carried out, they do offer a number of advantages that might be of tremendous importance to our ability to "surge" collection assets. They would be cheaper to build and to launch and could provide an extremely useful "on the shelf" reserve to increase collection during a specific crisis.

- **RECOMMENDATION: Development of more flexible collection capabilities should not only include moving to smaller satellites, but also to developing and incorporating "tactical" satellites that would allow for a "surge" in collection capability for specific crises.**

IC Centers and Task Forces

The utility of Centers include the capability to pull together quickly the disparate resources of the IC into a concentrated, synergistic effort on a specific issue or area. Because this structure can benefit the IC overall, a better ability to develop and operate Centers at a Community level should be developed. Centers will never be fully considered as "Community" assets as long as individual agencies believe that Centers are just a means of sacrificing resources with little or no specific benefit to the agency itself. Thus, a means of allowing the DCI to address personnel, budget and management issues for Centers, and shift resources accordingly, would benefit the Centers' effectiveness. The enhanced IC-wide personnel authorities given to the DCI (see *Intelligence Community Management* study) should increase the ability of the senior IC managers to use their personnel better to meet unexpected needs. This enhanced authority should be expanded so that he can go outside of the IC when necessary and should be used in conjunction with the DCI's authority to establish IC Centers and Task Forces quickly as a means of coordinating IC-wide resources for these needs.

- **RECOMMENDATION: The DCI's ability to establish IC Centers and Task Forces quickly (including the rapid transfer of personnel and resources throughout the IC) must be enhanced and should include the ability to bring "surge" resources into the IC from other areas.**

As important, the DCI must have the ability to quickly disestablish a Center or Task Force when its existence is no longer warranted and to guarantee that the contributing offices recover their assets. A review and evaluation process is needed to periodically assess whether a Center or Task Force is still a viable component.

Analytic Tools

The means for improving analytic capabilities will come with continued development of computer and information technologies and communications capabilities that foster better, more accessible relations among analysts. The ability to "surge" analytic resources through "virtual" means will be critical.

- **FINDING: Current efforts to create a Joint Intelligence Virtual Architecture (JIVA) within DoD show potential, and should be fully pursued and expanded upon to create a "virtual analytic environment" within the IC.**

Civilian Reserve Program

The development of a Civilian Reserve Program may be the most important aspect of preparing the IC for the future, especially in terms of linguistic and analytic capabilities. Fully developing a relationship with linguists, especially those in "exotic" languages, could fill significant gaps that are developing in the SIGINT and all-source areas of the IC.

The CIA already has in place procedures whereby it can increase its capabilities by using former employees on a temporary basis. This capability should be augmented into an IC civilian reserve program, to include experts not in the IC (in academia, business, etc.) who can be kept on retainer both to provide ongoing information on warning and trends and to be utilized during crises to augment IC assets. Such a program has several advantages. First, it allows the IC to concentrate on the current areas of concern while knowing that someone who is attuned to IC needs is also keeping an eye on areas that are quiescent. Second, the ability to bring in experts who understand local politics and players in a region is especially important during the early phase of a crisis, when the IC is often scrambling to come up to speed. Many of these experts can be kept on retainer and be asked to do unclassified work, which, in effect, will provide the IC with more knowledgeable access to the open sources. If the "reservists" are asked to work within the IC for extended periods, then some thought has to be given to the issue of clearances and polygraph requirements. A flexible approach to these issues would best serve the overall interests of the IC and the nation.

There are many ways a civilian reserve program could be run. To be successful, however, such a program would probably have to be developed and managed at the Community level, so as to properly address administrative concerns (security, pay, etc.) as well as substantive concerns -- assuring that duplicative expertise is minimized and agencies do not compete for resources to support individual reserve programs. Some developmental work on a reserve program is being done at this time in the National Intelligence Council (NIC). This work should continue and a pilot program should be enacted in the near term.

- **RECOMMENDATION: An IC-wide civilian reserve program should be established, whose participants can provide ongoing trends and warning information and can be utilized to "surge" as part of the IC, thus augmenting existing IC assets, especially during crises.**

Military Intelligence Reserve Resources

Similarly, better use should be made of military intelligence reserve components. Currently, reserve units are under the control of military service reserve chiefs who are responsible for ensuring necessary units are available for mobilization. By treating intelligence units strictly as mobilization assets, these units have been subjected to resource cuts and constraints as are any other reserve units. Additionally, any consideration of utilizing intelligence reserve units during non-crisis periods has evoked cries of Title 10 authorities and endangerment of military readiness. But intelligence is most effective for national security when it can deliver predictive analysis and warning well ahead of a crisis. Thus, it seems somewhat short-sighted to hoard capability that might be used to both prevent a crisis and certainly to prepare for a crisis, for the sake of ownership or control. Consequently, the Study Team believes that the SECDEF should capitalize on those efforts that are mentioned in this paper to craft an arrangement between the service reserve chiefs and the Director of Military Intelligence (DMI) to better utilize military intelligence reserve resources. This would result in allowing the DMI and DoD to make better use of intelligence reserves in non-crisis situations, thus adding an additional "surge" capability to the Intelligence Community.

- **RECOMMENDATION: Better utilization of existing military reserve components is also required. Consideration should be given to placing some of these components under the DMI for better utilization during time of need.**

INTELLIGENCE SUPPORT TO MILITARY OPERATIONS

Executive Summary

Support to military operations (SMO) is one of the major roles of intelligence. Some argue that it is *the* major role of intelligence. The Clinton administration -- both policy makers and senior intelligence managers -- has stated that SMO is *the* top priority for intelligence. Critics question why this statement is necessary, given that much of the Intelligence Community's (IC's) effort has always been shaped around this specific intelligence role and that, in the post-Cold War world, U.S. national security is actually less threatened than at any time since 1940.

This debate over SMO is important as it goes to the heart of both requirements and resources. Intelligence is not an easily expanded resource. As noted in the discussion on the IC's ability to surge (See the *Intelligence Community "Surge" Capability* staff study), covering current requirements and taking steps to address unexpected ones is difficult at best. The more resources devoted to any one area, the fewer there are left to address others. The issue is not whether the IC should devote resources to SMO, but rather how much SMO is reasonable given other, competing demands on a fiscally constrained IC.

SMO is, to some extent, a contingent need. At least through the Cold War, U.S. defense policy had been shaped around the idea of deterring combat, of using force as a last resort. Other, non-SMO, policy needs are current -- diplomacy, narcotics, terrorism, proliferation. Thus, a balance needs to be struck. Urging an increased emphasis on SMO without looking across the board at all IC requirements runs the risk of leaving many other ongoing policy needs partially or completely unfulfilled.

The IC has, in most cases, performed admirably regarding SMO. But the significance of the changes in our nation's national security "threats" and our responses to them, in how the nation employs its military forces, in the advances of technology on information processing, in the possible new paradigm in military strategies for combat, etc., that are either here or are on the horizon, suggests that extensive planning and operational, structural and management changes will be required for the IC to meet its overall national security needs, including SMO. Some of the findings and recommendations in this and other *IC21* studies go toward this end and need to be addressed soon if the IC is to be ready for the 21st century.

INTELLIGENCE SUPPORT TO MILITARY OPERATIONS

Scope

At the beginning of the *IC21* process, the Study Team was overwhelmed with the emphasis that was being placed on the issue of Support to Military Operations (SMO). This Intelligence Community (IC) "call to arms" was somewhat disturbing in that the vehemence that was expressed suggested that there was a crisis immediately at hand -- which was difficult to understand given the fact that our nation is less threatened, at least from a military perspective, than at any other time in the last 50 years. Were someone outside of the IC to hear the emphasis placed on SMO, they would likely come to one of three conclusions: that SMO was the top priority issue for intelligence, but that the IC had strayed too far into other areas and, now, needed to refocus; that the IC had experienced a critical failure in supporting the military and that extra efforts were required to fix the problems; or that, in a less threatening environment, intelligence demands had somehow dramatically increased for the military.

As there was at least marginal evidence that suggested that any of the aforementioned conclusions could be correct, we decided to specifically concentrate on current and future SMO as a separate study in *IC21*. The primary focus, however, was not on specific or detailed SMO requirements, but on how those requirements fit into the overall question of the roles and functions of a 21st century IC. Thus, this study centered on the following questions, at a macro level:

- Should SMO be the highest priority issue for IC resources now and in the future?
- Is the IC properly addressing SMO today?
- Are there indications that SMO requirements either have changed or will change in the future? If so, to what degree might this effect the priority for SMO in IC operations?

Consequently, this study did not focus on evaluating specific programs or assessing whether specific theater collectors were valuable investments. We did intend, however, to discuss some of the relationships between intelligence assets within the military, at all levels, and national intelligence assets, and how that relationship might change over time.

Approach

This study looks across the spectrum of issues facing the IC in SMO in the 21st century. The SMO Study Team conducted several interviews and panel discussions with retired and active intelligence professionals and military officers. These included "operators," some of the Commanders in Chief (CINC) of U.S. Combatant Commands and some military "theorists," such as Admiral William Owens, former Vice Chairman of the Joint Chiefs of Staff, who foresee very different types of military tactics and strategies than those that maintain our nation's defense posture today.

Along with the issues and questions raised above, the effect of the trends coming out of Desert Storm and the historical evolution of SMO, especially in terms of budgets, programs, operations and service equities, were studied as we assessed the IC's future challenges in this area.

What is SMO?

One of the questions from the beginning of the study was the definition of SMO. The role of SMO and, thus, defense intelligence is defined with variance, depending upon the forum. For some, it is solely an issue of support for the operational commander in a tactical wartime setting. Certainly, most of the discussions related to SMO since DESERT STORM (and, arguably, most of the emphasis) are aimed at improving our capabilities to support a similar effort in the future. In fact, some believe that *the* priority for reorganization of our intelligence capabilities should be to plan for capabilities that would support the military requirement to be able to engage in two, near-simultaneous "major regional contingencies" (MRCs). However, the continued growth of so-called "other military operations" (OMO) -- peacekeeping, peacemaking, humanitarian efforts, etc. -- that are putting U.S. personnel into harms way much as if they were in combat, call for different intelligence priorities overall and clearly indicates that the two MRCs concept is not an adequate planning tool for the IC.

Analytic and production elements of the military intelligence complex define their responsibilities by discussing the three "pillars" of support: support to the defense policy maker; support to force modernization and planning; and support to the warfighter. The individuals that make up these "pillars" would be, respectively: the Secretary of Defense (SECDEF) and other Department of Defense (DoD) policy makers; the Secretaries and staffs of the military departments charged with organizing, training and equipping the armed forces; and military commanders, planners and operators planning for or engaged in military operations. Although much broader than some definitions, this approach to the needs of the military by the IC is probably the most valid. Regarding support to the Secretary of Defense, since the end of the Cold War, the DoD clearly has become more prominent in U.S. foreign policy initiatives, even over the Department of State in some cases. From implementation of Nunn-Lugar

programs to promote Russian defense conversion to the deployment of troops into Bosnia to implement the Dayton Agreement, the DoD is the active arm of policy development and implementation. In part, this is due to changes in the stability of many regions and relationships that tend to involve armed entities and are a byproduct of a less polarized but more unstable world. For this reason, it is easy to see why much of the emphasis within the IC on SMO and "support to the warfighter" currently carries the day in terms of resource priority and focus. However, although DoD may be the active arm of many of the Nation's policy initiatives today, most if not all of these initiatives began with some level of diplomatic effort, calling into question whether "support to the diplomat" might be a more critical pursuit.

Support to force modernization and planning is also critical. Although some argue that this is less significant now that the Soviet Union no longer exists and strategic nuclear systems are being produced and deployed at a rate less than at the height of the Cold War, the facts are that Russia (and China) continue to produce strategic nuclear weapons and, most importantly, advanced conventional weaponry and defensive systems that will have an effect on U.S. force planning for years to come. Moreover, the sales of such systems to countries throughout the world by many countries, including Russia, underscore the importance of this type of intelligence to our weapon designers for protection of U.S. forces in the future. Another reason for emphasis on this type of intelligence area is opportunity -- more and more systems and technologies are available for purchase at arms sales throughout the world. Consequently, dedicated efforts by U.S. intelligence and defense to acquire previously hard to get equipment are especially important for the next 10-15 years. The Study Team believes that today's efforts in the Foreign Materials Acquisition and Exploitation (FMA/FME) areas -- currently managed under Office of the Secretary of Defense (OSD) and the Defense Intelligence Agency (DIA) -- are not as effective as they could be in order to assure that we capitalize on upcoming opportunities. The current FMA and FME programs tend to be piecemeal -- especially in terms of funding -- an issue that the Committee will continue to monitor with the FY97 budget submission.

"Support to the warfighter" is the area of main interest for DoD and the IC at present, and tends to be used interchangeably or as synonymous with SMO. The use of the term "support to the warfighter" is extremely problematic. It is misused to self-justify programs and budgets, and misunderstood, or defined so broadly as to encompass everything that the military does. It is also self-limiting, in that it promotes the immediate needs of a soldier, sailor, airman, marine or weapons system, making intelligence only a reactive function rather than a predictive one -- at a time when predictive analysis is becoming increasingly significant for the military commander as well as the policy maker. Moreover, the term suggests that the primary focus of intelligence should be on the actual need to use force (i.e., "fight a war"), when we continue to believe that successful foreign and national security policy is designed to preclude such an event if at all possible. This is not to say that the IC and the military

should not prepare for military conflict. But this cannot be the sole focus, to the detriment of diplomacy, deterrence and force preponderance -- all of which also require IC support.

Additionally, the current emphasis on "support to the warfighter" is primarily technologically oriented. In this burgeoning age of information, there seems to be a growing belief that technology will fix everything. "System compatibility," "interoperability" and "it's all bandwidth" appear to be the approaches that have become the focus for a majority of those -- including the services themselves -- who are bent on solving the "intelligence" problems for the military. Although clearly very important, having the ability to transmit volumes of data in near-real time has greatly overshadowed (in terms of interest and expenditures) the importance of the utility and availability of the information being passed. While striving to attain technical solutions, we must also address the intelligence data/analysis itself, as it, too, is critical to a commander's success. The current trends in priorities, however, suggest that the IC, and the military services, could go down the path, once again, that results in significant technological capabilities -- especially in collection assets -- with limited utility based on a lack of attention to processing, analysis and production capabilities. There is also the issue of the IC's ability to ensure that its information can be received by operational units and other intelligence entities. Dissemination, especially within a military theater, was a key intelligence issue in DESERT STORM. Whether this is a legitimate responsibility of the IC or of the military is a topic of discussion in a separate *IC21 Intelligence Communications* staff study.

This study, then, focuses on SMO mostly in terms that are associated with the third of the three "pillars." The Study Team believes that the issues of supporting the defense policy makers and force modernization and planning are as important as "support to the warfighter." This last "pillar," however, is likely to have the most dramatic effect in the future in terms of budgets, personnel, organization and priorities. In this study, given the limitations and misuse of the term "support to the warfighter," the issue of SMO is defined as those intelligence needs that support deployed forces. The Study Team believes that this support clearly should begin well before actual deployment and is not limited to traditional combat -- taking into account OMO and recognizing that a new paradigm in combat engagement is beginning to be realized. Likewise, as we need to consider new situations for the use of military forces, we must also review the "traditional" aspects of the intelligence information that is required for SMO.

Traditional SMO-related intelligence requirements -- that are still in use -- would include information on the size, capabilities and locations of a country's military forces, and physical details about a country's topography. This information is deemed necessary based on the possibility that U.S. forces may have to operate in a particular country in the future. Given the increased use of the military in OMO since the end of the Cold War, however, the needs of the operational commander appear to be

changing in a way that tends to blur the distinction between SMO and "support to diplomacy." As Lieutenant General Patrick M. Hughes, Director, DIA, testified to the Senate Select Committee on Intelligence (SSCI), "Threat ... is no longer a self-evident term. The defense intelligence community has traditionally focused on a primary element of the threat -- enemy forces and weapons systems; clearly that aspect remains. But as military activity extends to missions involving the use of military forces in non-traditional roles, we must adapt our intelligence focus to meet new requirements."

SMO vs. Support to the Policy Maker

As stated earlier, SMO is one of the major roles of intelligence. Some argue that it is *the* major role of intelligence. The Clinton Administration -- both policy makers and senior intelligence managers -- has stated that SMO is a top priority for intelligence. Critics question why this statement is necessary, given that much of the IC's effort has always been shaped around this specific intelligence role and that, in the post-Cold War world, U.S. national security is actually less threatened than at any time since 1940.

This debate over SMO is important as it goes to the heart of both requirements and resources. Intelligence is not an easily expanded resource. As noted in the discussion on the IC's ability to surge (see the *Intelligence Community Surge Capability* staff study), covering current requirements and taking steps to address unexpected ones is difficult at best. The more resources devoted to any one area, the fewer there are left to address others. The issue is not whether the IC should devote resources to SMO, but rather how much SMO is reasonable given other, competing demands.

Therefore, it is difficult to rationalize comments from senior IC officials (who also believe that a two MRCs defense strategy is sufficient for intelligence planning) who state that, "If you solve all of the military's requirements for intelligence, you will have solved 80 percent of overall intelligence requirements," as an acceptable blueprint for the IC today, let alone in the 21st century. Indeed, it is becoming obvious that, on any given day, the remaining 20 percent of the requirements could be more vital to the President and his policy advisors in areas that directly go to this Administration's stated principals of its national security strategy of enhancing security, promoting prosperity at home and promoting democracy.

Much of today's emphasis on SMO is directly related to supporting tactical combat situations. If one assumes that, on any given day, all of the other issues requiring intelligence support are more likely to be active than is the probability that U.S. forces will be in combat, then many aspects of SMO become an *insurance* capability. Like all insurance, intelligence support for warfighting is something you do not wish to be without, but is something you also work very hard never to have to

use. When viewed in this light, there is a greater desire to put some sort of limit on the degree to which the warfighting function calls unremittingly upon intelligence resources. Again, the insurance analogy is apt: how do you decide how much insurance is enough without short-changing other needs, all of which place real demands on resources.

Further complicating the issue is the fact that military commanders are now becoming more aware and interested in thoroughly understanding the issues within their theater in terms that go beyond preparing for combat engagement. The continued use of the military as an active participant of U.S. peacetime foreign policy by engaging in OMO, has bolstered this interest. Again, as Lt. Gen. Hughes explained to the SSCI, "'Warning,' traditionally focused on Clausewitzian warning of attack, is becoming an increasingly complicated process. We must build and employ a flexible and adaptive military intelligence support system in order to meet the needs of large-scale military threats, while at the same time meeting the military requirements of non-traditional warfare and the new missions the U.S. military has assumed." Consequently, it can be argued that in the near future, the requirements that encompassed the "other 20 percent" will be as critical to the commander as it is to the policy maker, in order for the commander to identify the key "centers of gravity" within each country's infrastructure as they develop.

There are already examples whereby commanders' interests conflict with SMO requirements -- the IC reaction to Presidential Decision Directive - 35 (PDD-35). PDD-35 is designed to present the Administration's highest national security priorities, thereby providing the IC guidance for resource allocations, by establishing a "tier" structure. Unfortunately, but predictably, the IC is using PDD-35 to ensure that resources are being placed on the highest-tier issues, in many cases having little or no resources left for lower-tier issues. One example of the effect is, in fact, in the area of SMO. In many cases, SMO is the top collection priority (and in many cases the only collection priority) for lower-tier countries, based on the possibility that U.S. forces could, some day, deploy to that area. Other non-military requirements for these lower-tier countries, however, such as a country's political climate, economic structure and internal stability, are of much lower priority or not reflected as having priority. Moreover, the growing number of SMO requirements threaten to consume resources that could be used to address non-military requirements. (Additional discussion of requirements can be found in the *IC21* staff study entitled *Intelligence Requirements Process*.) As a result, the Community may spend more time gathering intelligence for potential SMO than for monitoring other developments that might aid in supporting diplomatic efforts to prevent a situation where deployment of forces would be necessary. Ironically, several of the CINCs expressed the desire to have the type of non-military information that was traditionally important only to civilian policy makers.

SMO -- certainly in the traditional sense -- is, to some extent, a contingent need. At least through the Cold War, U.S. defense policy had been shaped around the idea

of deterring combat, or using force as a last resort. Other, non-SMO, policy needs are current -- diplomacy, narcotics, terrorism, proliferation. Thus, a balance needs to be struck. Urging an increased emphasis on SMO without looking across the board at all IC requirements runs the risk of leaving many other ongoing policy needs partially or completely unfulfilled.

The extent to which intelligence priorities must be balanced was suggested by Assistant Secretary of State for Intelligence and Research, Ms. Toby T. Gati, again to the SSCI. In describing what she called a second kind of threat to our national security -- the first kind being made up of issues such as terrorism, proliferation of weapons of mass destruction, organized crime, drug trafficking ethnic and religious hatred, the behavior of rogue nations and environmental degradation -- she stated that, "Such threats [the second kind] derive from missed or unexploited opportunities to advance our national agenda. If we fail to recognize such opportunities, or pursue them with ill-founded and misguided strategies, we can exacerbate existing dangers or create new ones. Intelligence can play a vital role in identifying opportunities for diplomatic intervention and provide critical support to our nation's policy makers as they seek to resolve problems before they endanger U.S. citizens, soldiers, or interests, and as they negotiate solutions to festering problems. This is the essence of 'intelligence in support of diplomacy,' an often ignored but vital component of our national security."

Clearly, then, striking the balance between SMO and other requirements is critical. Understanding how an administration views the use of the military and of the IC becomes a significant factor in the equation. In this Administration's national security strategy documentation (*A National Security Strategy of Engagement and Enlargement*), several points relating to these issues are addressed. On the issue of the use of military forces, the strategy begins by pointing out that, "Our strategy calls for the preparation and deployment of American military forces in the United States and abroad to support U.S. diplomacy in responding to key dangers -- those posed by weapons of mass destruction, regional aggression and threats to the stability of states." There is also a description of three basic categories of national interests that can merit the use of our armed forces:

> "The first involves America's vital interests, that is, interests that are of broad, overriding importance to the survival, security and vitality of our national entity -- the defense of U.S. territory, citizens, allies and our economic well-being."
>
> "The second category includes cases in which important, but not vital, U.S. interests are threatened. That is, the interests at stake do not affect our national survival, but they do affect importantly our national well-being and the character of the world in which we live."

> "The third category involves primarily humanitarian interests. Here, our decisions focus on the resources we can bring to bear by using unique capabilities of our military rather than on the combat power of military force."

Such guidance provides a broad flexibility in the use of military forces -- each requiring both varied and specific types of intelligence support.

Providing a view toward the importance and needs for intelligence, this same strategy calls for strong intelligence capabilities that protect our national security by "providing warning of threats to U.S. national security, by providing support to the policy and military communities to prevail over these threats and by identifying opportunities for advancing our national interests through support to diplomacy." Additional comments from this strategy include:

> "Because of the change in the security environment since the end of the Cold War, intelligence must address a wider range of threats and policy needs."
>
> "... its [the IC's] analytic effort must provide a coherent framework to help senior U.S. officials manage a complex range of military, political and economic issues."
>
> "U.S. intelligence must not only monitor traditional threats but also assist the policy community to forestall new and emerging threats..."
>
> "The collection and analysis of economic intelligence will play an increasingly important role in helping policy makers understand economic trends."
>
> "In order to forecast adequately dangers to democracy abroad, the intelligence community and policy departments must track political, economic, social and military developments..."
>
> "Finally, to enhance the study and support of worldwide environmental, humanitarian and disaster relief activities, technical intelligence assets -- especially imagery -- must be directed to a greater degree toward collection of data on these subjects."

Although no one will disagree with the concept, also in the strategy, that "Whenever U.S. forces are deployed, the highest priority is to ensure that our military commanders receive the timely information required to execute successfully their mission...," some balance needs to be considered. With the proliferation of military deployment throughout the world, mostly for OMO, a sole emphasis on SMO threatens to consume entirely IC resources to the point that the IC is only accomplishing SMO, thus, leading to a foreign policy that is almost totally reactive, with its primary response being the deployment of troops. This is a direction that the Study Team

believes is ill-conceived, short-sighted and not necessarily a path that this, or any, President should go down.

Clearly it is envisioned that the focus of the IC today needs to be on predictive analysis on a wide variety of issues of importance to the policy maker. As President Clinton stated when visiting the CIA in July 1995, "Unique intelligence makes it less likely that our forces will be sent into battle, less likely that American lives will have to be put at risk. It gives us the chance to prevent crises rather than forcing us to manage them." We would argue therefore that, although there will always be changes on the margins regarding details and descriptions of "threats," the premise that the IC needs to focus on the ability to provide "warning" on a variety of issues to the policy maker is an enduring top priority into the 21st century, one that must be addressed regardless of an immediate crisis, including military deployments. To accomplish the task of providing such warning, the IC will need to develop and maintain an extensive intelligence "base" of knowledge that is worldwide. Such an intelligence "base" should cover all aspects of a country, issue, or entity, with an eye toward being able to supply trends and warning data to the policy maker before a crisis occurs. (An intelligence "base" is also discussed in the *IC21* staff study on *Intelligence Community "Surge" Capability*.)

Finally, although the debate is often framed in terms of competing requirements -- SMO vs. support to the policy maker -- the trends indicate that priority toward the policy makers' needs is complementary to the needs of the operational commander in the 21st century. Again, evoking the words of Lt. Gen. Hughes, "Understanding military threat is a direct function of intelligence of all types: economic, political, environmental and, specifically, military, brought together in a dynamic all-source portrayal of overall conditions and circumstances. Understanding the military threat paradigm of the future will include not only traditional intelligence practices, but also a new approach to the threat including a recognition of the changing nature of the operational environment." To the extent that the "operational environment" is more than just the battlefield, and given the uses of the military for OMO since 1989, we would suggest that it is, we would concur with Lt. Gen. Hughes' outlook.

- **FINDING: The current demands being placed on the IC to support military operations will make it difficult for the IC to meet the broader national security challenges of the 21st century.**

- **FINDING: Currently, SMO demands are being satisfied at the expense of maintaining the necessary intelligence "base" that will be critical to the IC in addressing future national security needs.**

- **FINDING: Maintaining both the "base" and SMO represent valid concerns. SMO requirements must not stand alone, apart from other intelligence requirements.**

- **FINDING: The IC must develop and maintain a balanced approach in satisfying these concerns. The IC must ensure that the "base" is maintained even during periods of crisis, when IC resources can easily be overwhelmed by all consuming SMO requirements.**

Is the IC Properly Addressing SMO Today?

Assessing whether the IC is properly responding to the military's needs is a difficult question to answer, as there are varying levels of support that can be addressed. As the previous section of this study pointed out, the Study Team does not believe that the current direction of intelligence priorities, and the resulting management of IC resources, will adequately support the policy maker nor the military commander in the future. Other areas to consider would include whether the structure and operations of the IC, especially within Defense, properly support the military's needs in peacetime, during OMO and during combat operations.

Intelligence activities by the United States have a history that is closely linked to the military, sometimes exclusively. Indeed, the reasoning behind the founding of the CIA was to collate the disparate pieces of information that the individual military services, primarily, and other agencies (such as the Department of State) collected, and guarded zealously, so that the information could be useful to the policy makers as well as the government as a whole. But, guarding service equities has always been a key component of defense intelligence -- a component that has not changed even with internal military moves toward "joint" operations brought about by the Goldwater-Nichols Department of Defense Reorganization Act of 1986.

Although the Study Team did not intend to evaluate existing IC agencies regarding how they were performing, we could not help but notice that continued protection of individual services' equities and the lack of a strong defense intelligence focal point for policy and execution is causing the creation of a myriad of task forces, working groups, boards and committees that tend to try and attack new challenges while defending the structural *status quo*. Moreover, in order to make the existing rigid, vertical bureaucracy of the IC more responsive to the military, legions of representatives from intelligence agencies and program offices, and intelligence support teams now deploy to the theaters to provide SMO while, in essence, protecting structures. We certainly believe that, at the lowest operational level, a thorough understanding of and experience with the requirements of an individual service unit in the field must be part of the process of assessing needs, and, in some cases, having tactical intelligence assets controlled and operated in support of military operations is a requirement. This should not, however, be translated into "ownership" of assets in every case, and the "band-aid" structure that has been developed does not allow for the type of end-to-end, "corporate" approach that we believe will be needed.

This is not to say that improvements have not been made or that intelligence cannot support current military operations. Clearly, the overall status of SMO since DESERT STORM has improved in many areas. The successful management of delegated intelligence production by DIA, the establishment and operations of Joint Intelligence Centers (JICs), especially in the Pacific Command, to consolidate collection and analysis for the theater, the successful deployment and integration of unmanned aerial vehicles (UAVs) into theater operations to compensate for limitations of national collectors, the myriad of types of products produced by DIA specifically in response to operational needs and the establishment of the INTELINK system and the ability to access products on INTELINK via the Joint Worldwide Intelligence Communications System (JWICS) and the Joint Deployable Intelligence Support System (JDISS), are but a few examples where the IC, especially in defense, are responding to the call of new challenges in SMO. The old specter of redundancy and duplication have also been significantly reduced, and, although there may be additional areas where further attention to this issue is warranted, the redundancy that remains appears to be valid and healthy, as one all-source product cannot always serve all of the customer needs and requires some tailoring.

But the fact that the IC is coping with the challenges of Somalia, for example, and, now, Bosnia, does not indicate that current operations and structures are adequate for future SMO requirements. Several points in this regard were obtained through the research for this paper and can be further expanded upon.

The significance of military deployments for OMO, such as in Somalia, is that, in many ways, this type of support is more difficult and demanding than the traditional force-on-force analysis. This is because the military's requirements in this setting often call for more information on the immediate "environment" to which U.S. forces are engaged. Issues such as a population's dialects, religion, ethnicity and physical environment quickly become important for completion of the mission and for protection of our forces -- especially smaller ones. The types of arms and militia structure, if any, involved, that often do not conform to traditional force structures, are also vitally important. Likewise, understanding the more traditional military capabilities and operations of lower-priority countries continues to be important -- especially given the proliferation of weapons of all types -- and requires analysis before a crisis emerges. This was made painfully clear during DESERT STORM when assessing the IC's inability to locate and target Iraqi SCUD missiles and launchers -- an issue that was generally listed as an "intelligence failure." The truth is, however, that prior to DESERT STORM, the IC and the U.S. government did not consider the indigenous production of SCUD missiles to be a priority issue -- certainly not of enough priority to focus the required amount of attention and resources that would have provided a full understanding of SCUD operational deployment strategies. These factors specifically point to the growing importance of developing and maintaining an worldwide intelligence "base" of knowledge. This type of information is best supplied as the U.S. is approaching the decision to deploy troops -- indeed, it should be

factored into the decision-making process. As stated in the previous section, maintaining this "base" of knowledge must continue regardless of a crisis at hand. This "base" of knowledge need not be in the Defense intelligence area -- many of the types of information may be better analyzed in CIA, for example -- as long as Defense has ready access when needed. (Also see the discussion of the intelligence "base" in the *Intelligence Community "Surge" Capability* staff study.)

The establishment of JICs addressed the realization that the operational commander did not understand, nor had the time to deal with tasking national collectors. One of the often heard comments to the Study Team was that the collection "stovepipes" forced a commander to place multiple requests for information, each uniquely structured so as to fit into the specific collection discipline. Moreover, the development and employment of National Intelligence Support Teams (of which there are at least four supporting Bosnian SMO), JICs and Joint Analysis Centers (JACs) and the Defense Collection Coordination Center (DCCC), further indicate that better "horizontal" and synergistic management and operations of national collection assets is required. (See the *Intelligence Community Management* staff study and the *Collection Synergy* staff study for further discussion and for recommendation to create a Tactical Collection Agency.)

A growing concern about the concept of "sensor-to-shooter" was also expressed. Although some types of information need to be sent directly to a weapons system, inundating and overwhelming the "warrior" is a decided possibility. Some saw the eventual solution to this data overload problem in enhancing the capabilities and responsibilities of the JICs and JACs for data/analysis fusion. Others were still concerned that the prospect of turning the "warrior" into an analyst, and, thus, reducing his operational effectiveness, were real and not necessarily good.

- **FINDING: Emphasis on concepts such as "sensor-to-shooter" have promoted the dissemination of intelligence data and products to the lowest level of military operations, without full consideration of the effect on the "warfighter."**

The issue of interoperability of information systems between the IC and the military and between individual services is still an issue. A comment from a study of Bosnian operations last year by the Defense Science Board summarized the issue, "The multitude of separate, stovepipe, stand alone systems has proliferated in the theater by well meaning providers." This has caused, "unnecessary overlap and has overcomplicated fusion." (See the *Intelligence Community Management* staff study for a recommendation to establish an Infrastructure Support Office.)

The concept of Command, Control, Communication, Computers and Intelligence (C4I) is, at best, an artificial construct. Intelligence is a user of communications and is, in fact, becoming more closely integrated with operations. Tasking, collecting,

analyzing, fusing and disseminating intelligence useful to the commander and the "warrior," and providing the mechanisms (communications), especially within theater, that allows for the necessary dissemination in the time required are two different and daunting tasks. Realization that the integration of national and tactical collectors will also be key to future SMO has caused the military to add emphasis on integration of collectors for Intelligence, Surveillance and Reconnaissance (ISR) to enhance battlefield information. The difficulty in developing inter-theater and cross-service compatibility with enough available bandwidth to support operations is a difficult task; one that has been the primary focus of the Assistant Secretary of Defense (ASD) for C4I. Integration of ISR components and ISR with operations is, in many respects, no less difficult, requiring more focused senior-level attention than it is currently given by the ASD (C4I). (See the *Intelligence Community Management* staff study and the *Intelligence Communications* staff study for a recommendation for an Assistant Secretary of Defense for Intelligence.)

The advent of information technologies is having an impact on intelligence reporting and dissemination that bring about significant management challenges. Although DIA has taken great strides in managing analytical and production responsibilities within DoD, technology that allows for more collaborative production will further blur the "lanes of the road," and will likely result in significant challenges ahead. Some of these challenges from a system perspective are being addressed in the development of INTELINK and the Joint Intelligence Virtual Architecture (JIVA). From an intelligence analysis and production perspective, however, there is a growing concern that single-source (collection discipline) publications are increasingly using collateral information to help put their information into context, thus, appearing more like all-source publications. As a result, users may well incorporate a piece of analysis into a tailored report for the commander that is believed to be a product of all-source analysis when it is not. As technology allows for easier publication possibilities by more and more users of INTELINK, the problem can be exacerbated. The IC as a whole, but, specifically, DIA will need to take a more prominent management role.

Finally, given the disparate responsibilities and activities of intelligence throughout the defense establishment and the fact that intelligence can take only a small portion of the SECDEF's time, there needs to be a senior military officer responsible for military intelligence management; someone who can look at defense intelligence from "end-to-end," and also allow the DCI to obtain the "corporate" view of the IC that will be required. (See the *Intelligence Community Management* staff study for a recommendation of establishment of a Director of Military Intelligence.)

Future Requirements for SMO

Perhaps one of the more interesting dynamics that will significantly affect SMO for the future is the explosion of new technologies across a wide range of disciplines and the emergence of truer "joint" warfighting resulting from the Goldwater-Nichols

Act. The culmination of these points, observable in some limited fashion during DESERT STORM, has some within the military discussing new concepts in warfighting that could redefine SMO 10-15 years from now. Such concepts envision an information-reliant battlefield environment in which intelligence plays not only a significant role, but a dominant and directive one. An example of this is the concept of providing a commander with "Dominant Battlespace Awareness (DBA)." As defined in the *Annual Strategic Intelligence Review* on SMO, this concept is:

> "... the capability to achieve real-time, all-weather, continuous surveillance in and over a large geographical area. This capability should be sufficient to determine the presence of most objects, emissions, activities or events of military interest. The awareness portion of the concept is not limited to enemy activities -- it includes awareness of friendly forces, weather, terrain and the electromagnetic spectrum. The battlespace over which the Joint Force Commander establishes DBA includes the geographical area (surface, subsurface, atmosphere, and space above it) where the most intense conflict will take place. DBA is not solely an intelligence function."

Such goals, combined with the new challenges being contemplated in the area of Information Warfare, pose daunting challenges for the IC -- from both a technological and analytical standpoint -- and there are only few who likely fully understand the ramification for the IC and for the military. Moreover, the excitement associated with these concepts could easily overwhelm the intelligence planning and support process so that development is concentrated in these areas to the detriment of other national security needs. Some would argue that this "militarization" of intelligence is already underway with the current leadership in the IC.

What is true, however, is that in DESERT STORM, the introduction of advanced, precision strike weaponry, the identification of critical "centers of gravity" within the Iraqi infrastructure and the tactical requirements for information throughout the conflict pointed to a shift from intelligence as a contributor to intelligence as a participant. Lt. Gen. Kenneth Minihan describes this shift as akin to the roles of a chicken and a hog in a ham and eggs breakfast. In such a meal, the chicken is a contributor, while the hog is a participant. Although mired in traditional force-on-force strategies and operations, DESERT STORM represented the beginning of a shift for the military in how future wars will be fought. It also deftly portrayed the all-consuming nature of conflict on intelligence, especially as a participant.

To effectively provide SMO in the 21st Century, the IC will likely have to develop a concept of "Dominant Awareness." The ability to be active in collection and analysis -- ahead of immediate requirements -- will make the IC our first line of defense. The ability to maintain a knowledge "base" on an extremely diverse set of countries and issues will not only help protect broad national security objectives, but in OMO, it could well save lives. In tactical, combat situations, taken to the logical

extremes projected by concepts such as DBA, intelligence must somewhat take the lead rather than only providing a more traditional supporting function that is often reactive. To the extent that the military moves in the direction of DBA, specific cultural changes must be made, by the military and by the IC, in how intelligence is collected, analyzed, disseminated and used.

Support for the type of battlefield, or battlespace, that the military is planning to operate within will take significant steps, especially in automation, to achieve. Put simply, a capability must be developed that provides continuous, near-real-time, sensor-to-shooter data on all targets and all weapons. Such a capability begins with collection capabilities. The ability to operate "national" and "tactical" collectors in near-real-time and in a synergistic fashion that does not waste resources, based on redundancy or system limitations, is critical. The speed at which these systems must react suggests that not only an integrated tasking mechanism must be developed, but that at least some significant portions of such a system needs to automated -- operating without the burden of human intervention. Likewise, the experience already gained from Bosnia, indicates that extensive, quick-reaction theater collectors and innovative "national" collection capabilities must be developed to meet many of our future needs. Finally, a robust HUMINT and clandestine SIGINT program is also of key importance. Having the "person on the ground" will continue to be the best way to assess an enemy's intentions. This type of collection support must begin well before troops are deployed and the battle begins. Waiting until the U.S. establishes military "presence" will not provide the information and advantages needed.

Analysis and dissemination in this type of SMO environment must provide the capability to identify the "centers of gravity" of an enemy's infrastructure, and to have a thorough understanding of the enemy's "environment" prior to the beginning of a conflict. The ability to fuse intelligence data -- not only the "raw" data from collectors, but also disparate analysis from theater and "national" entities becomes especially important so that the tactical field commanders are not inundated to the point where their efficiency and effectiveness are diminished. On the battlefield, the ability to fuse intelligence data and provide a real-time picture of legitimate targets is a necessity. Such a capability may not be obtainable without significant advances in automation to assist in areas such as bomb damage assessment.

Today, systems development in the areas of ISR are primarily in the hands of collection program managers in the NRO and the acquisition components of each individual service and OSD. If the IC is to meet the needs of the military in the future, a more "corporate," end-to-end outlook and management structure for the IC as a whole will be needed. In the 21st Century, the IC must attain a "dominant awareness" of worldwide activities, without waiting to be asked, if it is to provide the predictive and proactive type of intelligence that will make it relevant to the policy maker and the military commander.

- **FINDING: The new operational strategy, Dominant Battlefield Awareness, will require significant advances in technology, development of consolidated requirements, coherent tasking management and synergistic intelligence collection capabilities. It is necessary to give serious thought to the amount of IC resources likely to be available to support such strategies.**

The Study Team firmly believes that SMO is a vital part of the intelligence role and mission. The IC has, in most cases, performed admirably in this regard. But the significance of the changes in our nation's national security "threats" and our responses to them, in how the nation employs its military forces, in the advances of technology on information processing, in the possible new paradigm in military strategies for combat, etc., that are either here or are on the horizon, suggests that extensive planning and operational, structural and management changes will be required for the IC to meet its overall national security needs, including SMO. Some of the findings and recommendations in this and other IC21 studies go toward this end and need to be addressed soon if the IC is to be ready for the 21st century.

INTELLIGENCE CENTERS

Executive Summary

The purpose of this study is to examine the seven existing Intelligence Centers, assess their effectiveness, the need for these Centers in the future, and whether the Centers "concept" can be adapted as a working model for future Intelligence Community organization. The study will also make recommendations on how to improve the functioning of the Centers.

There are seven centers: the Counterterrorist Center, the Counterintelligence Center, the National Counterintelligence Center, the Crime and Narcotics Center, the Nonproliferation Center, the Arms Control Intelligence Staff and the Center for Security Evaluation. All the Centers are located in the Central Intelligence Agency headquarters buildings in Langley, Virginia. The Centers were established to serve as "Community" organizations. In reality, they have a distinct "CIA" identity. They are predominantly staffed by CIA employees, and are dependent upon the CIA for administrative support and funding -- often competing with other CIA programs for resources. This fact has made it difficult for the Centers to be accepted as "Community" entities.

At the outset, Centers must overcome bureaucratic impediments and require a significant period of time to mature as organizations and establish themselves as full players in the Intelligence Community. Much of the success of Centers can be attributed to the quality leadership the CIA has selected for service in the Centers. In this study, we considered where the Centers should be located in the Intelligence Community. Also examined were the factors that have made the Centers successful, and the problems that continue to trouble them -- geographic barriers, bureaucratic inertia and personnel management impediments.

We concluded that, in most respects, the Centers have become successful, established organizations that should continue to exist. In fact, in many respects, they are now indispensable, representing the type of functional outlook and horizontal integration of analysis and collection that will be critical in addressing the complex transnational issues of the future. Our study recommendations include improvement on community management issues, the need for periodic functional review, and a number of suggested changes to the personnel system.

INTELLIGENCE CENTERS

Why Were Centers Created?

The Centers were established to serve as focal points for significant and enduring intelligence issues. They function as vehicles to pull together the disparate intelligence resources on major issues in order to provide more synergistic collection, analytical and management approaches toward a critical intelligence problem. They also allow the Intelligence Community to show its responsiveness on major issues to the Administration and to Congress.

The Centers work because they have established valuable, even essential roles in the Intelligence Community. Specifically, the Centers were created to meet certain perceived needs, and over the years they have made themselves viable entities -- although not necessarily as true "Community" centers with full Community staff representation, as initially envisioned. What the Centers have done is meet the objectives that had been set forth for them and become valued Agency and Community resources. Moreover, they are organizations upon which policymakers have come to rely.

The Centers -- What Are They Now?

Today, the Centers continue to address specific issues identified by their names. They draw, with varying degrees of success, from personnel throughout the Intelligence Community. Indeed, the very name "Center" implies a certain degree of Community orientation, or that the center is a "shared Community resource." In reality, though, most of the Centers have a distinct "Central Intelligence Agency (CIA)" identity, are predominantly staffed by CIA employees and depend on the CIA for their administrative support and operating expenses.

In a sense, the very name "center," is also misleading. The Centers are not true cross-agency organizations, and they are not always the single focal point for work on an intelligence issue. In the case of the Nonproliferation Center (NPC), for example, three National Intelligence Officers (NIOs) also speak on various aspects of nonproliferation. Moreover, the Director of Central Intelligence (DCI) Community Nonproliferation Committee, although chaired by the NPC Director, is a separate coordinating entity. Of all the subject matters upon which Centers have been formed, proliferation is probably the most diverse across the Community. It can range from Measurement and Signatures Intelligence (MASINT) research and development (R&D) to analysis on export regimens. In this area, probably more than all others, it is beneficial to have a Center that can provide a centralized planning and coordinating function for the Intelligence Community and between intelligence and policy. It is interesting that the role of the DCI's Nonproliferation Committee is set forth in a DCI

Directive. By contrast, there are no DCI or other directives that institutionally identify the corporate intelligence authorities and responsibilities of the NPC. In fact, although it should be a DCI entity, given its function, the NPC is contained within the CIA's Directorate of Intelligence (DI).

Each Center has unique features and, therefore, it is difficult to generalize regarding their roles and missions. It is possible, though, to group the seven centers into two generic categories. The Center for Security Evaluation (CSE), the Arms Control Intelligence Staff (ACIS), the National Counterintelligence Center (NACIC) and the NPC most closely approach what might be called Community coordination mechanisms. The Counterterrorist, Counterintelligence, and Crime and Narcotics Centers (CTC, CIC and CNC, respectively) are more the Community's operators. They contain fused DI/Directorate of Operations (DO) line elements that directly support certain intelligence activities.

The Centers were intended to be shared Intelligence Community resources with substantial representation of staff from elsewhere in the Intelligence Community. This has not occurred. What the Centers have become, though, are central repositories of information related to their assigned subject matter. Other agencies, to varying degrees, have come to rely on the Centers' data. How the Centers differ from the National Intelligence Council (NIC), another repository of all source analysis, varies from Center to Center. In some, the difference lies in the sheer number of staff who work with the intelligence issues. For instance, the NPC can do more than the NIC in looking beyond the immediate uses of intelligence to assess trends as well as policymaker, analytical and collection needs. Yet, actual analytical work on proliferation issues is performed outside the Center. Other Centers such as the CIC, CNC and CTC are central repositories and producers of analytic product and at the same time are closely involved with operational activities. Another way to describe a Center such as the CTC is that it is like a DI/DO partnership into which a Community partnership is inserted as well. The CTC has close-working analytical and operational components, but considers itself the "one stop shopping spot" for intelligence support to planning and execution of U.S. counterterrorism policy in all its forms.

Where Should the Centers Be?

As the former CIA Executive Director, Leo Hazlewood, describes it, the worst thing about the Centers is that they are CIA centers and the best thing about them is that they are CIA Centers. For years, the chief complaint from within the Intelligence Community was that the Centers are "CIA" centers. By this, the critics meant that because the Centers were located in the CIA, it followed that their focus would be weighted too heavily toward CIA interests. As a result, according to the critics, other Community needs would get short shrift. There were also concerns over turf, with some Community program managers feeling threatened by what may be perceived as an infringement upon their responsibilities. Of course, similar complaints regarding turf

have been voiced from within the CIA. It is not surprising that these complaints were especially intense during the Centers' formative years. The complaints and critics have not entirely disappeared. Nonetheless, we have found that despite their CIA location and large CIA staffs, the Centers, in varying ways, have made great efforts to incorporate and accommodate the information, needs and interests of the entire Intelligence Community and, by and large, they have succeeded.

-- There have been problems. Some of the more conspicuous deficiencies relate to the Counterintelligence Center's information sharing practices with the FBI and others in the Intelligence Community. The creation of the National Counterintelligence Center, with its substantial FBI and community representation, as well as the assignment of an FBI Agent to a senior position in the DCI Counterintelligence Center, has greatly improved the flow of information between the FBI and the CIA.

When Leo Hazelwood says that the best thing about the Centers is that they are CIA centers, he means that of the entire Intelligence Community, the CIA has been the one intelligence agency willing to make the resource investment in these "Community" Centers. The Centers were initiated by the CIA and have been staffed primarily by its personnel. With the exception of ACIS, CSE and NACIC, the Centers are located in the Operations or Intelligence Directorates. The CSE and NACIC are located in the Community Management Staff (CMS). From those organizations, the Centers derive administrative support. It is argued that this support can be factored into their budgets at a significantly lower cost than if they required separate infrastructures, either outside the Directorates, or even outside of the Central Intelligence Agency. Administrative support may be more expensive if provided by the DCI budget; if the Centers were entirely outside the CIA and other intelligence agencies, their infrastructure costs would be higher still as they would be unable to borrow or ride on any common services or networks.

Moreover, according to the CIA Comptroller, it is easier to protect the Centers against unallocated cuts and/or personnel reductions if they are located budgetarily within a larger directorate, such as the DI, where there is a large pot of money, some of which can be shifted to protect priority projects. In the current budget structure, outside the cushion afforded by a larger program, they would feel the full brunt of unallocated budget reductions. Both the present and former Comptroller felt strongly that taking the Centers out of the Directorates, therefore, would be a mistake. Any "independence" from organizational "taxes" on Center budgets or constraints imposed by directorate viewpoints would be of small benefit compared to increased vulnerability and the added operational expenses that independence would mean.

It is interesting that of the Center Directors interviewed in this study, those who felt comfortable in their relations with the directorates and saw no benefit in relocating their Centers outside the larger organization were Directors of Centers within the

Operations Directorate. Other Center Directors were troubled by the number of times they had to give up resources to the interests of the Intelligence Directorate in which they resided and felt their Centers should be made independent, or had succeeded in becoming independent of that Directorate so that they would not continue to lose funding and personnel to other programs. One Center had managed to get itself moved outside of the Intelligence Directorate for just this reason.

Looking Forward

Taking these arguments for budgetary protection into account, discomfiture remains about the vulnerability of the Centers to the interests and funding objectives of the directorates in which they reside. The protection against unallocated cuts is a persuasive argument, but it assumes reductions will continue, and that the Centers cannot be protected in any other manner. In addition, those Centers that reside within the CIA's Intelligence or Operations Directorates will continue to draw criticism for being CIA entities. Finally, we believe that the Center concept presents the right direction for future management on major issues, but only if their structure presents the right sense of corporateness. The study, therefore, concludes that the best solution is to relocate as many Centers as possible out of CIA directorates to where they can be perceived as having the most "Community" flavor. It is possible, however, that this may not mean out of the CIA as envisioned in *IC21*. (See the *Intelligence Community Management* staff study.)

What Makes Centers Work?

For Centers to become fully functioning in today's Intelligence Community, they need time to establish their place in the intelligence bureaucracy, they need the leadership and commitment to make them work, and they must readily adapt their structure and activities to remain relevant.

Centers Need Time to Mature

It takes time for a Center to become effective. Forming a Center to address a Community issue in a centralized way does not mean once the Center is "stood up" that the Center mission is fully functional. Consistently, those interviewed in this study felt that Centers needed time to mature as organizations and to establish themselves as viable institutions within the intelligence bureaucracy. Some have suggested that this process takes a minimum of five years. Even those tasked with getting the newer Centers running, and who thoughtfully sought to apply lessons learned from the struggles of older Centers, discovered that, despite their best efforts, they seemed bound to a five-year "principle."

DCI Directives can establish a Center in name, and will outline the Center's mission and responsibilities. Only time and effort can make a Center, functionally, a

Community Center. If one also takes into account the administrative expense of setting up new offices and transferring the personnel to staff it, one understands that establishing a Center is not a short-term solution.

Centers Need Good Leadership

It seems a given that the successful director of a new Center must become involved in struggles over bureaucratic turf. Establishing new relationships requires sheer force of personality and excellent personal relations skills. In addition, the directors must be able to support their employees both within and without the Center. All Center employees are detailees. Centers are faced with a common perception that career advancement can be slowed by assignment to a Center. Overcoming that perception so that good quality staff will be attracted to the Center is important to any Center's overall success. Thus, all of the directors have found it necessary to go the extra mile to support employees in the personnel review process. In the future, reforms to the personnel appraisal process may relieve some of the burden on the directors by providing a clear process by which employees can be evaluated for "out of directorate or agency" contributions. These reforms will be discussed in greater detail at a later point in this study.

Centers Must Be Flexible

Due to their own initiative or, as a result of change imposed from outside, the Centers have had to respond quickly to change or, if need be, to reinvent themselves. Centers, like all organizations, run the risk of becoming stagnant or behind the times. The Centers must change their organizational structures and activities in a timely way to be able to demonstrate their continued importance, a factor that is of great importance to Centers, as they are the natural competitors with line organizations.

Although interviews with Center personnel revealed a commitment to keeping their organizations flexible and able to change, in reality, changes requiring additional funding and personnel may be impeded by the needs and interests of the larger organization in which some of the Centers are presently located. There have been a number of occasions when the Centers in the Intelligence Directorate have had to give up funding for other Directorate needs. On the other hand, Directorates have given up personnel and funding to augment Centers with missions the Directorate felt were of utmost importance. This has been most noticeable in the Operations Directorate. Taking these histories into account, the study concludes that flexibility in Center programs might be best achieved if the Centers were placed in a separate Community account that would subject them to fewer competing interests. Flexibility might also be enhanced by a "seed monies" account. Over the past few years, "seed money" provided to the Centers has helped the Centers initiate certain technological developments throughout the intelligence community.

Looking Forward

The need for time to become established, the need for good leadership, and the ability to change are essentials that are required now for Centers and will be in the future as well. Again, looking into the future, there are some factors that may diminish Community resistance to the Center concept. Resistance to Centers appears primarily in the form of bureaucratic turf battles or, on a more personal level, negative perceptions about the impact of out-of-directorate (or agency) detailing upon one's career. The future should bring improvement to these problems as, over time, the number of people who have served in the Centers grows. Interestingly, although downsizing has an adverse impact on the ability of Centers to obtain personnel from other agencies, it has a positive effect on the Center efforts. Computer automation developments such as joint data bases, congressional pressure to reduce duplication, and relaxed compartmentation standards have provided the impetus to work more joint activities, with a resulting increase in intra-agency assignments. Downsizing has also pushed short-staffed agencies toward greater cooperation and teamwork. Another factor operating in the Centers favor is that, as time goes by, there will be an ever growing number of people who have served in the Centers and have returned to their respective agencies with a more "corporate outlook." These factors, and the resultant impact on the milieu in which the Centers find themselves, will not change in the foreseeable future.

No matter how well-led and flexible a Center organization might be, like any organization it is in danger of becoming self-perpetuating. As part of their coordination effort, Centers frequently establish new working relationships where none existed before. This is one of the great benefits the Centers offer the Intelligence Community. However, once these processes become established, it may be appropriate for the Center to disengage and permit the activity to continue without Center involvement. In order to encourage disengagement when it has become appropriate, and, as an overall review of roles and missions, we recommend that a five-year review process be required of each Center to assess all ongoing Center activities and to rule on the need for its continuation.

Barriers and Impediments to Making Centers Work

There are three kinds of barriers to making Centers work. The first barrier consists of the problems inherent in establishing a Center's role in the Intelligence Community and the attendant turf issues. These problems have already been discussed.

The second barrier is a physical one relating to the far-flung locations of the intelligence agencies. This geographic reality can be an impediment to detailing employees among the agencies. It is a lot to ask a National Security Agency (NSA) employee who likely lives in central Maryland or Baltimore to commute to Langley, Virginia for two years. The geographic barrier and the turf barriers are issues that must be resolved by leadership and management. It might be useful to consider a reimbursement policy for detailees who must travel distances significantly different from what they normally would encounter.

The third barrier is a large set of institutional and bureaucratic rules governing employee movement, evaluations, and security. It is in the realm of personnel management that the Centers face some of their most nettlesome problems. It is in this area that this study will make the majority of its recommendations. Like the geographic barriers, some of these obstacles can be mitigated by creative and committed management that provides strong direction and incentives. Others can and must be changed not only to improve the efficacy of the Centers, but to facilitate cross-agency working relationships in the Intelligence Community of the 21st Century.

Getting Good People to the Centers

One of the perceptions that has plagued the Centers is that there have been cases where they have been used as places to send underachievers. Early on, the belief was that managers were sloughing poor performers and problem employees off on the Centers. Busy with turf battles and establishing their own roles and missions, Center directors at first did not give their attention to the quality of personnel. However, the directors and the Agency itself have given more attention to this problem in recent years, and there have been improvements.

Several years ago, as part of an overall review of the Counterintelligence Center, the CIA Inspector General examined the promotion rates and performance of the Center staff. The IG found the Center was filled disproportionately with poor performers. They also found that the Operations Directorate had been the primary culprit in giving poor performers to the Center, not the Intelligence Directorate. An Inspector General study of the Counterterrorism Center done last year compared the promotion rates of those assigned to that Center to those serving in the Directorates. They found the DO had the greatest problem with promoting personnel who had served in the Centers, all other valuative factors being relatively equal. In yet another study, the CIA Executive Director's staff gathered personnel statistics on the Centers and found that the Counterintelligence Center stuck out from the other Centers in having a disproportionate number of people who had not advanced in their careers at a normal rate before coming to the Center.

Additionally, in 1993, the former DDI, Doug MacEachin, and ADDI, Dave Cohen, did a review of DI personnel detailed outside the Directorate, to include rotations in the Centers. Looking back over a period of years, they found that the percentage of people on rotational assignments outside the Directorate was steadily increasing. Their study also found that 40 percent of the people whom the DI had in rotation fell into the lowest performance percentages. The proportion of poor performers was even higher in the Centers. As a result, the ADDI issued an order that no one in the bottom tenth percentile could be sent to a Center unless the career service, the Center director and the individual in question agreed that they should go.

Each of the Center directors are aware of the problems of perception and/or fact that working in a Center is not career enhancing. All have taken a more aggressive role in the PAR process and, with the exception of the NPC, all Centers have a vote on the promotion panels. Recently, the CIA Executive Director has decreed that no senior level assignments are possible without an "out of directorate" experience. If Directives such as these count rotations to Centers as an "out of directorate" experience, they may, to some degree, help alleviate concerns about the impact of Center rotations upon promotion rates. Until employees are comfortable that their promotion rates will not suffer when they are out of the sight of their home division, the perception that service in a Center can be detrimental to one's career will not fade away. This perception can only be changed by tangible results. We are encouraged by the current Executive Director's interest in personnel management reform; many of the problems highlighted above are now under review. Such reform, however, needs to be injected into the Intelligence Community as a whole, as "out of directorate" rotations alone will not serve the Centers adequately.

From the Centers' perspective, any reform of the personnel evaluation procedures within the CIA must include a process that would provide more efficient and fair evaluation of the contributions made by employees detailed to Center or "Community" positions. That evaluation should be meaningful to the division or directorate to which the employee belongs.

The DO has a central personnel system in which the Directorate evaluates its employees across the divisions. In the Intelligence Directorate, on the other hand, each Division is essentially its own personnel stovepipe. The division personnel systems were formed to track the development and contribution of analysts focused on a specific issue area. The focus on contribution to the division coupled with the number of personnel "duchies" in the DI makes it difficult to evaluate employees as directorate, Community or Center resources. As increased numbers of analysts are working details outside their divisions, the DI has responded by creating a rotational groups panel to improve the evaluation process. However, this is a patchwork-type response where a more sweeping change to the evaluations of DI employees may be called for.

The study proposes that the DI's personnel system be changed so that it can continue to facilitate the development of junior analysts, but also more effectively evaluate intra- and interagency contributions made at a more senior level. One way this might be done is that employees up through the GS-12 level would be evaluated by their home division. From the GS-13 level onward, personnel would be evaluated by a Directorate-wide panel. Such a panel may be better poised to incorporate into its reviews criteria relevant to the entire Directorate, as well as overall Agency or Intelligence Community interests.

The problems Centers face regarding the evaluation of detailees' contributions point to a more sweeping issue -- how analytical personnel of the 21st century should be evaluated. Today's analyst spends a great deal more time on short-term reporting and "corporate" projects than analysts of past years. Yet, the system that evaluates analysts still leans toward a "publish or perish" or "what have you done for the division lately" mentality.

The "out-of-sight, out-of-mind" problem can be a career threat for an Agency employee on rotation outside his or her directorate. The problem is even more acute when detailees come from other agencies whose evaluation criteria and procedures may be significantly different. Therefore, it is not surprising that Center directors who are aggressive in seeing that good CIA employees are recognized and rewarded, are less effective with supporting workers who come from outside the Agency. Presently, the NPC and the CTC, two Centers that have taken on military detailees, are struggling, for example, to find a way to make their evaluations of performance coherent and meaningful to DoD military evaluation criteria.

Additional Personnel-Related Problems

Another suggestion that was brought up frequently during this study was the need to reform the CIA's Personnel Assessment Report (PAR) process. Too often PARs are put together by managers less as an evaluation of an employee than as a package designed to get someone promoted.

The Centers presently possess a mixture reimbursable and non-reimbursable billets. In fact, the same is true of many offices or groups throughout the Intelligence Community that have detailees from other agencies. The issue of reimbursable versus nonreimbursable billets must be explored further, for it is possible that a Community-wide policy of reimbursable billets might make loaning personnel to Centers or other agencies less burdensome, particularly for the Defense Intelligence Agency (DIA), which must count that detailee against numbers remaining in DIA offices.

Although work is being done on developing Community security policies, certain policies are not consistent across agencies. From the Center perspective, many object to the imposition of CIA security regulations that are imposed on Center staff, especially polygraphs. This impedes getting detailees to serve on the Centers.

The "Virtual" Center

Conventional wisdom is that there is no substitute for people working together, face-to-face. Nonetheless, there remains a sense that the advent of common data bases across agencies, video conferencing capabilities and other forms of electronic communications -- not the least of which the secure telephone and fax -- might make it possible, for example, for counterterrorism offices of different agencies to work as a virtual center from their desks in their respective agencies. Yet, try as we may, it is hard to subtract the human contact equation and come up with a dynamic, workable model. To establish a new organization, develop a new cross-Community cooperative process or focus on quick moving issues like terrorism requires intensive, face-to-face interaction. It is true, however, that Centers can and do establish new working relationships that are facilitated by Community data bases and video conferencing. Once these working relationships are established, the Center itself may no longer be required.

Imagery Management and the Centers

Several years ago, the NPC assumed the role of the nonproliferation imagery manager for the Intelligence Community. In reviewing its management efforts, the NPC did a comprehensive review of imagery requirements against worldwide weapons of mass destruction targets. As a result of their work to improve management of the imagery deck, the Center found a more than three-fold increase in meeting nonproliferation imagery requirements.

The CNC uses imagery to support its counterdrug efforts. In working with DEA, the CNC provides that agency with imagery where needed. As this relationship began, the CNC found that the DEA agents could not understand the imagery process. In response, the CNC established a Counternarcotics Imagery Working Group that would interpret imagery used to assist the DEA. In addition, an agreement was worked out making the CNC the Executive Agent for imagery counternarcotics targets, much in the same fashion as the NPC is the Executive Agent for nonproliferation targets. The CTC staff is concerned about how its efforts in this area will be affected by the formation of the proposed National Imagery and Mapping Agency (NIMA).

Task Forces

One area of consideration in this study was the relationship between Centers and Task Forces. The similarities between the two are striking, although the functions, structures and duration of the two differ. A number of Task Forces have been created to respond to specific regional problems, such as the Balkans, or to focus on certain issues, such as strategic planning or Community management. The Task Forces resemble to Centers in that they bring synergy to a Community that is fragmented. Here again, the Task Forces are a response to an Intelligence Community that is finding a corporate approach to problems both necessary (due to shrinking staffs and funds) and beneficial. Unlike Centers, Task Forces are formed presumably for short-term, *ad hoc* problems -- although the fact that the Balkans Task Force has been in existence for over three years suggests that "short-term" is not always the norm.

Typically, Task Force assignments do not present the same personnel problems such as concerns about the adverse effect on one's career as a result of being detailed for two years to a Center. In general, work on a Task Force is viewed more favorably -- in fact, the attention one can receive for work on a short-term, attention-getting Task Force can be career enhancing. Yet, like Centers, Task Forces may incur administrative and bureaucratic burdens associated with assigning or moving personnel on a temporary basis. Depending on the structure of the Task Force, funding, interagency representation and space needs may also be troublesome. As with Centers, the issue is the "portability" of intelligence resources across the Community and the ability to "surge."

We believe that Task Forces, like Centers, serve important functions for the Community. To be effective, however, Task Forces need to be highly focused on specific, short-term issues, and their continuation should be monitored, perhaps on a yearly basis, to ensure that they remain responsive to answering the needs of the specific problem or issue for which they were established. Finally, because of the short timelines that would, in part, drive the formation of a Task Force, additional DCI authorities that allow for shifting resources within the Community must be available, and acceptance by the Community and the government of a Task Force as the DCI's/Community's authoritative body for that crisis must be assured without delay.

Centers in the 21st Century

Many of the observations and recommendations in the previous paragraphs relate to changes that should be considered, given today's Intelligence Community. The overriding question, however, is how the concept of Centers relates to the type of activities the Intelligence Community will need to conduct in the 21st century. We believe that Centers (and Task Forces) are valuable components of the present Intelligence Community, and that Centers will continue to be worthy organizations on

into the 21st century. The "Center" meshes with our overall concept of a more "corporate" Community that capitalizes on a more synergistic approach to collection and analysis, and the interaction of these two activities.

As pointed out previously, there are two basic types of Centers. We believe that this distinction will, and should, continue, as each type highlights particular strengths regarding how intelligence is used. As transnational issues become more complex, coordination of operations throughout the Community (and the government) will be a major key to a Center's success. Of note is the ground broken by the NPC in its interaction with the policy process. Although in some cases its activities have been to fill voids in the process, NPC's operations specifically point out the utility of intelligence in aiding the decision making process without specifically directing the outcome (or the policymaker's decision). While the military is finding that intelligence needs to be fully integrated into operations to achieve so-called Dominant Battlefield Awareness, the same type of integration into the policy process will be no less important.

Finally, the NPC director's role as an issue manager has also broken ground. Congress directed that NPC develop a report that takes a functional, issue-based look at the overall intelligence budget for the FY96 submission. The House Intelligence Committee found the report to be a useful tool in understanding the Community's efforts on proliferation issues, that we believe it will be a mainstay approach for the future. Although some have qualms about some of NPC's activities, such interaction and overall resource focus may well define the type of analytic and management activities the Community will need to adopt across the board in supporting the 21st century policymaker and intelligence planner.

In order to achieve the type of synergist operations and corporate mentality that will be required in the 21st Century, the Intelligence Community will have to significantly adjust its practices regarding personnel, security, resource management and other issues that are seen as specific barriers that are found when observing each agency within the Community. Resolving these problems is especially important for the success of the Centers. Some specific proposals and recommendations regarding these areas can be found in the *Intelligence Community Management* staff study. Generally, however, we find that Centers should be the corporate answer to major transnational issues, and should be managed as such.

In the other *IC21* studies, we redefine the role of the CIA as the Intelligence Community's premier all-source analysis and production entity. As such, this seems like the appropriate place for most of the Centers. However, it is clear that Centers should represent the DCI and the Community and, consequently should be directly controlled by the DCI, the Deputy Director of Central Intelligence or, perhaps, the Director of Military Intelligence, and not in some CIA substructure.

Findings and Recommendations

1. **The Centers are successful, established organizations that should continue to exist.** The Centers were created to address critical, enduring intelligence issues; these issues will continue to be important to U.S. national security for the foreseeable future.

2. The Centers are in daily contact with the entire Intelligence Community as it relates to their subject matter. Because of their responsibilities, they keep current with all aspects of their topic, relevant policymaker needs and requirements, the contributions of the various Intelligence Community programs with which they work, and problems related to gaps and capabilities. **Thus, we find that Center directors are best choice for issues managers, in that they are, for the reasons stated above, best suited to do the "racking and stacking" across the Community of programs and resources.**

3. **The Centers fall short in being the Community organizations they were intended to be.** A critical shortcoming of today's Centers is not the work they do, but their less-than-Community composition. Greater Community representation in the Centers will help diminish the perception that they are "CIA" Centers. Greater Community representation also would improve the lines of communication between the Center and the rest of the Intelligence Community. **We believe that greater Community representation on the Centers would help diminish the perception that the Centers are "CIA" centers and result in improved communication, information sharing and cooperation among the agencies. Thus, there should be a commitment, if not a requirement, that the Community's leadership fill all of the Centers' Community billets. Increased Community staff participation in the Centers should be expected in the future.**

Management

4. **We recommend that a mandatory five-year review process be imposed upon the Centers to revalidate the continuing necessity for all of the seven Centers' missions and activities. This review will include strong consideration of the management of high-priority requirements across the Intelligence Community and the Centers' contribution to the plans and activities designed to meet those requirements.**

5. There are serious questions to be asked about the Nonproliferation Center that go less to its contributions -- which have been significant -- than to its future form and function. It is unclear what pieces of proliferation management should be the purview of the NPC. Since 1993, Congress has been adding to the powers of the NPC while, at the same time, CIA managers have reduced its authority, personnel and budgets. **We believe the issues management responsibilities should be returned to the NPC, but that all other NPC activities should be subject to an immediate validation review.**

6. It takes years for a Center to achieve a viable role in the current intelligence bureaucracy. The lesson to be drawn from this is that a Center or a center-like structure may not be the best organizational response to a short-term crisis. The DO, for example, is turning more and more to the task force process to work crises. There are many similarities between task forces and centers. In many cases, both must acquire office space, move employees and establish cooperative working relationships with existing IC offices. **If task forces are being established to perform as mini-centers, they may not be the best or only solution to short-term problems. In fact, increased information automation and joint conferencing capabilities may make physical collocation of task forces unnecessary. Centers and center-like task forces (longer in duration) likely will continue to require collocation of personnel.**

7. **If the Centers were placed in a Community account, that program might also include some special Centers funding, including seed money, that could be used by the Centers to push Community response to special needs or new technologies.** There would be increased flexibility in planning, if that Centers special funding were placed into a multi-year account.

8. **The Intelligence Community should develop a consistent policy regarding reimbursable or nonreimbursable billets in the Centers. In many cases, reimbursable slots would encourage Community participation in the Centers. An appropriate amount of funds should be designated to fund reimbursable slots.**

Personnel

9. **The geographical distance between the agencies that might be represented in the Centers is a barrier to achieving full cross-community participation in the Centers. The study recommends reimbursement for the extra travel required of Center detailees if that travel exceeds 20 miles daily.**

10. Not only do the Centers find it hard to fill Community staff positions, they also face the perception -- and sometimes fact -- that service on Centers is not career enhancing. As detailed by the study, there are reforms to Community personnel management practices that would benefit the Centers. The Centers need assistance in getting qualified and productive detailees from within and without the CIA, and a means to assure that the detailees are fairly evaluated and their promotion rates are not adversely affected by Center service. **It is important that the evaluation process be revised to more fairly and accurately evaluate the contributions of the Center detailees and other detailees who serve outside their home office.**

11. In attempting to respond to the need for broader based evaluations, the DI has established a rotational assignments panel. It remains that the DI has as many personnel systems as it has divisions. **The study recommends that these personnel systems remain in place for the evaluation of employees below the grade 12 level. Above the grade 12 level, these systems should be replaced by a directorate-wide system which applies overall directorate standards and the measures developed by the rotational assignments evaluation process.**

12. **Personnel performance evaluations should shift their focus from skills to issues.** The National Photographic Interpretation Center (NPIC), for example, has gone to this model. They have grouped together technicians, analysts and others together and evaluate employee performance with regard the issue being worked. Where there used to be personnel structures for each skill category, personnel management has been more efficiently consolidated to an issue-focused process. Evaluation and personnel management conducted in this way would make it easier to evaluate the work of Center detailees and the increasing number of other intelligence employees working outside their home offices.

INTELLIGENCE AND LAW ENFORCEMENT

Executive Summary

For years, the intelligence and law enforcement communities have maintained an uneven, and at times an antagonistic relationship. This is due partly to differences in the roles and cultures of the two communities, as both have different responsibilities and objectives, as well as expectations regarding information acquisition and management, and because of differing end uses for that information. There have been other factors that have affected the interaction between law enforcement and intelligence. During the 1970's, investigations into improper domestic intelligence activities uncovered some degree of overreaching of intelligence into domestic areas. One of the results of these investigations was that the two communities tended to further distance themselves from one another over concern about further inadvertent missteps. Then, beginning in the late 1980's, two banking scandals (BCCI -- Bank of Credit and Commerce International -- and BNL -- Banca Nazionale del Lavoro) highlighted deficiencies in information management within and between the two communities. Investigators from Congress and the Intelligence Community itself recommended that problems relating to coordination and information management be remedied.

Several other phenomena have focused the attention of the Committee and others on the future relationship between the two communities. Over the past 10 years, a number of statutes have been enacted that expand the extraterritorial responsibilities of U.S. law enforcement agencies. Frequently, these laws require FBI activity in areas that also are of significant intelligence interest -- narcotrafficking, terrorism and proliferation of weapons of mass destruction. Another factor bringing the intelligence and law enforcement closer together in recent years is that traditional crime issues such as international organized crime, illegal immigration, money laundering are becoming intelligence topics as they increasingly are viewed by policy makers as threats to U.S. national security.

Although the two cultures differ in their rules, objectives, procedures, use of human sources and standards relating to the quality and quantity of information they collect, a number of procedures can be established to improve communication and coordination within the framework of existing directives and statutes. We believe that there is no need to further clarify the National Security Act of 1947, as amended, or the subsequent Executive Orders. There is a flexibility in these laws that permits a reasonable, but well-bounded, range of interpretation that will allow for improved cooperation and coordination between law enforcement and intelligence without blurring important demarcations between the missions and authorities of the two communities.

For the last two years, a careful interagency review of these intelligence/law enforcement relationships has been carried out by the Joint Task Force on Intelligence and Law Enforcement (JICLE). The JICLE has focused on legal policy, operations, information management and judicial support, and has developed recommendations and procedures in all these areas. The contribution of the JICLE in trying to resolve the many issues related to intelligence support to law enforcement is important; the growing coordination and cooperation between the intelligence and law enforcement communities is partly a result of the Task Force's efforts. Training will be essential to bring about better understanding differences in the two communities' objectives and methods, and in establishing procedures by which the two communities can interface effectively.

Of these many issues relating to intelligence support to law enforcement, this study has focused on the issues of tasking, crimes reporting, liaison, coordination of activities and assets overseas, oversight, limits on searches of Intelligence Community files, training and the reporting of law enforcement investigatory information to Congress. The recommendations made in this study focus on legislation, resource issues and overseas coordination.

INTELLIGENCE AND LAW ENFORCEMENT

Changing Scenarios

With the reduction in the Russian nuclear threat and a lessening of that nation's support for insurgencies around the world, the Intelligence Community has shifted more of its resources to focus on other problems of growing importance: proliferation of weapons of mass destruction; terrorism; drug trafficking and weapons transfers -- also topics of interest to the law enforcement community.

Although, some have argued that the end of the Cold War should have reduced the problems facing law enforcement and intelligence; in fact, the opposite is true. For example, the collapse of the Soviet Union about the breakdown of a degree of authoritarianism that had suppressed to a certain level the corruption and lawlessness in that country and its Eastern Bloc neighbors. These changes, as well as technological developments that have revolutionized processes for transferring information, goods and money, have helped to provide a fertile operational field for the transnational criminal.

In the past 10 years, drug trafficking and terrorism statutes have been enacted which expand the extraterritorial application of some aspects of U.S. criminal law. As a result, the numbers of law enforcement investigators abroad has increased. Law enforcement's expanded responsibilities overseas has led to a greater interest by law enforcement in Intelligence Community information, as well as the likelihood for interaction with intelligence communities overseas activities and responsibilities.

Parameters of Law

The National Security Act of 1947, as amended, specifically authorizes the Central Intelligence Agency (CIA) to collect intelligence through human sources and other appropriate means, except the CIA shall have no "police, subpoena, or law enforcement powers or internal security function." The intention of the law was to hold intelligence separate and distinct from law enforcement activities. At the time the Act was written, there was concern about creating a monolithic central security service that history -- and observations made of totalitarian states -- had taught us was undesirable in a democratic society.

Permissible intelligence collection activities were further clarified by President Reagan's 1981 Executive Order 12333. The order provided guidance to all intelligence agencies on the scope of allowable collection and other intelligence activities. Within the limits set out in the Order, the Intelligence Community is permitted to collect a large amount of foreign intelligence that is of interest to law enforcement. Section I.4c authorizes the intelligence agencies to undertake the

"collection of information concerning, and the conduct of activities to protect against, intelligence activities directed against the United States, international terrorist and international narcotics activities, and hostile activities directed against the United States by foreign powers, organizations, persons or their agents." Thus, the Order empowers the Intelligence Community to collect and analyze intelligence on the foreign aspects of traditional law enforcement concerns such as narcotics production and trafficking, international terrorism and counterintelligence.

Law Enforcement and Intelligence - Two Different Cultures

Even as the law enforcement and intelligence communities have increased contact due to overlapping interests, problems can arise relating to coordination and cooperation because the two communities possess different rules, objectives, different sources and methods, and different standards regarding the quality of information they collect. Traditionally, intelligence agencies collect political and military intelligence for policy makers; law enforcement investigators gather information for prosecutions. There are few rules governing intelligence gathering -- it generally involves activity abroad that is illicit or undertaken with the host government's covert cooperation and does not focus on U.S. citizens. By contrast, law enforcement focuses primarily within U.S. borders, territorial waters or airspace. In enforcing those United States laws having extraterritorial application, the law enforcement emphasis is upon crimes committed by U.S. nationals or upon illegal or foreign activities that affect U.S. national security, U.S. property or U.S. nationals. Law enforcement activity outside the United States and within other countries' borders is usually undertaken overtly in cooperation with the host government.

Further, the two communities have different expectations with regard to the information they gather. Law enforcement gathers information to build a case upon which criminals can be prosecuted and sent to jail. A criminal defendant is entitled, under the Sixth Amendment of the U.S. Constitution, to a speedy public trial. The Constitution guarantees a defendant notice of the charges against him, the right to confront his accusers, the right to counsel and the right to subpoena witnesses on his own behalf. Further, the prosecution must disclose to the accused any potentially exculpatory materials that it has in its possession. In public criminal trial proceedings, law enforcement information therefore should be unclassified, and reliable and accurate enough to establish proof beyond a reasonable doubt in a courtroom. (The 1980 Classified Information Procedures Act (CIPA) provides for certain pretrial, trial and appellate procedures for criminal cases involving classified information. CIPA is designed to take into account the sometimes competing needs of the prosecution, the constitutional rights of the criminal defendant, and the national security concerns of the Intelligence Community.)

In contrast to law enforcement, the Intelligence Community gathers tremendous amounts of information based on a complex set of needs and requirements established

by the policy makers it supports. This information can be collected simply to develop understanding of an issue, not necessarily in preparation for an action. Unlike law enforcement information, much of this data is of questionable reliability and obtained only on the understanding that it will not become public knowledge. The collected information is reviewed and evaluated by intelligence collectors and analysts who gauge its reliability and accuracy.

By contrast, law enforcement investigators and prosecutors obtain their case information from interviews, statements and affidavits from prospective witnesses, searches, physical or electronic surveillance, documentary information obtained for a variety of sources, grand jury proceedings and informants. Their investigative techniques must comply with constitutional mandates such as the Fourth Amendment's general prohibition against unreasonable searches and seizures and, absent circumstances fitting within specific exceptions to the general rule, its warrant requirement. Judicial decisions, statutory language, Attorney General guidelines and other internal directives may also clarify appropriate investigative limits and techniques. The statutory standards for physical searches and electronic surveillance in the foreign intelligence context differ from those applicable in a criminal investigation.

Law enforcement informant information can come from either long or short-term human sources. Long-term informants may be used to assist in a prolonged investigation of complex criminal activities or of a criminal organization, or they may be used for their assistance in more than one investigation. These valuable sources are seldom revealed in prosecutions. Instead, law enforcement investigators may develop informants whose contributions are expected to be more short-term in nature. These informants supply case-related information, and their relationship with law enforcement generally terminates when the case is closed. By contrast, human intelligence sources are almost all long-term assets recruited overseas by case officers. Additional intelligence comes from national collection capabilities that include imagery, communications and signals intelligence. These collectors gather a myriad of information -- but they are designed to be long-term capabilities to collect against certain types of targets. The key to their longevity is the understanding that they will not be compromised, such as could be the case if the information is used improperly in a law enforcement action or the source is required to testify before a grand jury or court.

Separation Between the Two Cultures

Over the past 50 years, the intelligence and law enforcement communities have operated in largely different spheres, separated by mission, culture, scope of activity and law. Several major changes have occurred within the past decade that have complicated this fundamental orientation of the two, pushing them further apart or closer together. In the 1970's, scandals that involved overreaching into U.S. domestic

areas by the Intelligence Community and improper domestic intelligence activities by the Law Enforcement Community were uncovered by the Watergate, Rockefeller, Church and Pike Investigations. A number of reforms came out of these investigations. One of the unwritten but significant side effects of these investigations was behavioral in nature. The years that followed the investigations were marked by some reluctance on the part of the two cultures to form interactive relationships. This over-caution was based more a perception that closer association meant increased political risk than having any basis in prohibition of law.

Since the late 1980's, several additional events have occurred that have led up to the changes in the relationship that are now occurring.

BCCI and BNL Cases: The Need for Better Intelligence and Law Enforcement Cooperation

In the late 1980's and early 1990's, there were two notable financial scandals of international dimension that highlighted problems with intelligence and law enforcement information management. In the BCCI (Bank of Credit and Commerce International) case, the CIA had used the bank for its own purposes, but also reported on the illegal activities of that organization. Investigators found the CIA reports were not made in a manner to focus law enforcement agencies on the violations occurring. A report on the BCCI affair made by two Senators to the Senate Foreign Relations Committee found that CIA analysts had failed to grasp the significance of the information they had before them as it related to violations of international banking law. Another finding was that CIA reports had not been provided to relevant agencies in a consistent manner.

In the BNL (Banca Nazionale del Lavoro of Italy) case, similar problems were uncovered. Over time, the CIA had developed a number of intelligence reports and analytical products regarding the BNL. When asked by investigators to produce a compilation of these materials, the CIA found it difficult to retrieve all relevant material in its various files. Moreover, what the CIA had provided to the Justice Department and others had been disseminated in an *ad hoc* fashion, a matter made worse by poor record keeping. For its part, the Justice Department was unable to retrieve records of the intelligence that had been provided to it by the CIA. The intelligence that had been provided by the CIA had been misplaced or forgotten until subsequent searches by both the Justice Department and the CIA uncovered material that probably should have been produced for the defendant or the court.

The findings of the Senate investigations of BCCI and BNL concluded that there was a need for better information management on the part of the CIA and the Justice Department. In its investigation of the BNL matter, the Senate Intelligence Committee also called for better coordination between the law enforcement and intelligence communities and for more and improved law enforcement access to intelligence files.

Congressional pressure for change and the growing recognition by both communities that, because of changing law enforcement jurisdictions and world developments, the two would be working in closer proximity to each other, prompted the formation of an interagency task force to work on these problems and other issues of concern. That initial task force, and the one that followed, found this job to be larger and more complicated than anyone had anticipated.

Interagency Task Forces

The first task force was begun in 1993, at the behest of then Director of Central Intelligence James Woolsey and Acting Attorney General Stuart Gersen. This interagency group was headed up by Deputy Attorney General Mark Richard and CIA's General Counsel, Elizabeth Rindskopf. The task force's mission was to consider the broad range of issues that affected intelligence and law enforcement community interaction and what measures could be taken to improve coordination, with particular focus on the problems brought out in the BCCI and BNL investigations. In August 1994, the task force issued a report that included 23 recommendations to improve coordination, including the establishment of liaison offices to provide prosecutors with a better understanding of what intelligence support is appropriate. Although the report concluded that both intelligence and law enforcement have "sufficient legislative and regulatory authorities to cooperate effectively," the task force did not provide concrete resolutions of coordination issues. Rather, it recommended that working groups be formed to continue to resolve the problems outlined by the task force.

In early 1995, several groups were formed to carry out the first Richard/Rindskopf recommendations. The Intelligence Community-Law Enforcement Policy Board was established in May to meet quarterly on issues of mutual concern to the Attorney General and the DCI. The Board is co-chaired by DDCI George Tenet and Deputy Attorney General Jamie Gorelick. Membership on the Board includes all of the law enforcement and intelligence agencies, the Assistant Secretary of State for Intelligence and Research and the Defense Department's General Counsel.

Two working level groups were established to report to the Policy Board. The first is the JICLE or Joint Intelligence Community-Law Enforcement working group. This group's job is to address the specific problems identified in the Rindskopf-Richard report. A second group, the Special Task Force on Law Enforcement-Intelligence Community Coordination, has the responsibility of developing guidelines for overseas coordination between the two communities.

Other Factors Push Intelligence and Law Enforcement into Closer Relationship

In the past few years, the physical and functional separation of law enforcement and intelligence has lessened. One impetus to a closer relationship has been deficiencies in information sharing brought out by the BCCI and BNL investigations.

But there are also other factors that have been pushing the two communities into a closer relationship. There has been a major shift in the world order that has taken place since the fall of the Soviet Union and the end of the Cold War. There have also been changes in law responding to transnational criminal activities that are increasingly affecting the United States.

The 21st Century World

The world of the 21st Century is one that will be increasingly interconnected. The speed of transportation, efficiencies in the movement of goods and the electronic transmission of information and money represent new mediums in which transnational activities -- legal or illegal -- can flourish. The criminal enterprises that will thrive in a globalized world will inevitably cross many nations' borders. More than ever before, law enforcement agencies are finding that crimes are being visited upon the citizens of one nation by the residents of another.

Some of the more significant criminal activities that are of greatest concern to policy makers are illegal finance activities (including money laundering), car theft rings, the movement of prohibited goods, precursor chemicals, nuclear, biological or chemical weapons, and illegal toxic waste dumping. In addition, crimes such as drug trafficking, money laundering and alien smuggling that were typically of national or regional effect only a few years ago now cause problems worldwide.

Growing Number of Extraterritorial Statutes

There is a limited inventory of federal extraterritorial jurisdiction that includes crimes committed aboard American ships or planes; offenses which imperil or misuse our foreign commerce with other nations; misconduct, like genocide, terrorism or air piracy; overseas theft or destruction of the property of the U.S. government; the use of violence against its officers or employees, or the obstruction or corruption of the functioning of its agencies overseas. Finally, there is federal extraterritorial jurisdiction over activities outside the U.S. that result in or are intended to result in harm within the U.S., such as drug trafficking. There are also state crimes that can have extraterritorial application. These vary from state to state and include misconduct such as theft, murder or conspiracy. State laws tend to be more detailed and restrictive in purpose and interpretation.

Why is International Crime a National Security Concern?

The internationalization of crime can create a security gap for any nation. The detrimental effects of crime can be proportionately greater in smaller nations, and particularly threatening to emerging democracies. For example, most nations today are struggling with fiscal deficits. Money laundering and other criminal activities compound debt problems because very large sums of money are lost as taxable

revenue. Corruption and bribery, caused by and causing criminal activities, can stand in the way of legislating effective enforcement laws. Corruption and illegal activities can stymie pro-democracy efforts because of the pressure debt problems can put on an economy and social welfare. Moreover, the presence of significant criminal activity can make it difficult for a nation to attract the commercial investment needed to make its economy grow. Thus, the inability of countries to deal with crime has a destabilizing effect; also, the criminal activities taking place within their borders can have a reach far beyond those borders.

In order to put the international wrong-doers out of business, all affected nations must be willing and prepared to enact and enforce laws that make it difficult for criminals to operate within their borders. For example, money launderers will do their worst where laws prohibiting illegal transfers of funds are lax and they can expect to escape scrutiny. They will also operate where corruption is prevalent enough to protect them from disclosure.

Transnational problems inevitably raise the issue of international cooperation as one means of response. It is interesting to consider the role of the State Department and law enforcement community in combatting international crime problems, especially as both are expanding into this area. In late 1995, the State Department renamed its Bureau for International Narcotics Matters (INM) to the Bureau for International Narcotics and Law Enforcement Affairs. At the time of the reorganization, a Deputy Assistant Secretary was designated to focus on International Crime and Policy Planning. This official is responsible for the development and implementation of foreign policy initiatives to counter international criminal threats to U.S. national interests and programs to strengthen criminal justice institutions in support of Administration of Justice/Rule of Law Programs. The State Department is urging better coordination between all entities of the Government that have an interest in international organized crime. For its part, the Justice Department is involved in a number of the Rule of Law Programs, which involve a variety of overseas training assistance activities. The law enforcement community generally has been supportive of the State Department's efforts to better coordinate these programs.

The growth in law enforcement's overseas presence and investigatory activities has produced a sharper debate over the roles of intelligence and law enforcement agencies overseas, with most discussion focusing on the degree to which the Justice Department will coordinate its activities with the Ambassador. The Justice Department has expressed a willingness to inform and coordinate with a designated embassy official regarding its activities in country. Indeed, such coordination is required by law (22 U.S. C. 3927). However, Justice draws the line at allowing any embassy official to become involved in prosecutorial decisions relating, for example, to whether a case will be pursued. Discussions on this issue are ongoing; a Memorandum of Understanding relating to coordination of law enforcement activities

overseas is expected sometime in 1996, as is a report from the Overseas Coordinating Group, whose task it is to resolve the myriad of coordination issues that can arise abroad.

Liaison/Coordination of Assets

In a recent statement, Deputy Attorney General Jamie Gorelick stated that the FBI intends to recruit informants and engage in operational activities overseas. There are varying opinions on the degree to which the FBI will be active in this area, as well as how broadly the term "informant" is to be interpreted. In reality, most law enforcement contact with informants is to be done openly, and with the knowledge and consent of the host government. As pointed out earlier in this report, use of informants is much a part of the FBI's criminal investigative repertoire. The Drug Enforcement Agency (DEA), an organization with a large cadre of officers overseas, also uses informants. Although relations have not always been perfect, by and large, where the DEA and CIA are both present in country, coordination between the two agencies has worked and should continue to improve. However, there remain a small number of instances where the FBI, in particular may become involved overseas with clandestine sources recruited in the U.S. In such cases, the FBI cooperation with the CIA on these activities is imperative, and efforts are underway on the part of both organizations to strengthen the conduct of these activities.

At a minimum, we believe that recruiting of and contact with confidential informants overseas by the law enforcement community should be coordinated through the Chief of Station. We recognize that to a great extent this is already being done, although not consistently. We understand that there will be criminal investigative activities occurring in areas that are not subject matter of interest to intelligence. In these cases, there may be benefit derived from law enforcement's use of intelligence information for contextual information, but coordination of activities themselves will not be a factor.

Increased FBI presence overseas has highlighted other issues relating to the relationship between the FBI and the CIA. For example, there has been some debate over the conduct of liaison with law enforcement and security services. Some have posited that the FBI should have sole responsibility for liaison with foreign law enforcement entities. The argument is that law enforcers relate best with other law enforcers, and the presence of CIA liaison raises the specter of possible recruitment attempts, which can have a negative influence on law enforcement cooperation. The FBI has argued that its reputation as a respected law enforcement entity could be tarnished should a CIA recruitment of a foreign security representative to go awry. DEA officials have also expressed concern that its law enforcement image might suffer in some countries should its association with the CIA become known. These arguments have some merit, but are not necessarily relevant where security and intelligence organizations are one in the same. Another factor that weakens the

exclusivity argument is that corruption is frequently a significant problem overseas. Given the focus of many law enforcement investigations, it might unwise to deny the CIA potential access to those who might inform on the nature and extent of corruption in their country. For these reasons, we oppose any effort to preclude the CIA from having liaison with law enforcement overseas, although there may be cases where it would be appropriate for the FBI to be the primary liaison. The CIA has a long history of involvement with overseas security organizations and should not be denied continued contact in this area. Basically, this is a problem that can be less settled by a commitment to careful coordination between the intelligence and law enforcement communities.

Just as law enforcement must have primacy regarding any transnational activity undertaken inside the United States, we believe the CIA should have local primacy in pursuing transnational issues in foreign countries. This means the Chief of Station must have full cognizance of law enforcement activities where intelligence interests may be affected, except where such information may be specifically denied him or her due to grand jury secrecy requirements as set forth in F.R.Cr. P. Rule 6(e), which precludes disclosure of matters occurring before a grand jury.

Searches of Files

One of the problems highlighted by the BNL and BCCI investigations is that intelligence was not conveyed to policy makers as thoroughly, meaningfully and consistently as perhaps it could have been. As discussed earlier, there were also flaws in the Justice Department's handling and management of intelligence information and reporting. As the interagency task force has sought to improve upon procedures relating to the provision of intelligence to law enforcement, two significant problems have arisen. The first questions to what degree intelligence agencies should (and can be) expected to report criminal activities to the Justice Department. The second information-related issue is the protection of intelligence files from exculpatory searches during the prosecution of a criminal or civil case.

Reporting Requirements

In 1982, a Memorandum of Understanding (MOU) between the Justice Department and the Intelligence Community established Intelligence Community obligations to report evidence of criminal activity relating to intelligence assets or information uncovered during the course of collecting for other intelligence requirements. In recent years, representatives from both communities had come to recognize that some revisions of the MOU were needed to reflect changes in law and policymaker interest.

In August of 1995, a new Memorandum of Understanding was approved. As before, the MOU requires the Intelligence Community to report suspected significant criminal misconduct by officers, employees, contractors or agents. Among other things, the MOU represents an attempt to minimize the number of special reports that will be required of the Intelligence Community. Because intelligence analysts are not experts in criminal law, and for other reasons stemming from the nature of intelligence information, we believe that reporting requirements should not include possible violations of law involving third parties acquired during foreign intelligence collection. This information should be disseminated as part of routine intelligence to law enforcement agencies. Considering the unfortunate experiences of both communities relating to BCCI and BNL, we believe that making the process more efficient should be one goal of the new MOU. There is also concern that intelligence analysts are not the proper people to review all information for potential criminal activity. Attempts to train or hire intelligence analysts to perform such functions may move the Intelligence Community into proscribed law enforcement responsibilities.

Unfortunately, it is almost inevitable that at some point some tidbit of information will be overlooked by the Intelligence Community or the recipient law enforcement agencies, creating to some extent a reprise of the "banking" case problem. In light of the vulnerability to post facto judgments regarding the significance of criminal-related information, recent problems relating to "criminal" activities of human sources, and the current debate over what reporting should be required of the Intelligence Community, we may wish to consider statutory or other language that will set forth "reasonable" expectations and goals in these areas. It also may be wise to require some form of periodic reporting to Congress on some of these matters.

Limits on Searches of Intelligence Community Files

In the overall intelligence/law enforcement relationship, serious problems can arise when, during the course of a prosecution, the defendant feels there is reason to believe there may be exculpatory evidence related to him or her in Intelligence Community files and requests a search and a Brady (Brady v. Maryland (1963)) ruling. Searches like these pose an enormous threat to intelligence sources and methods. Yet, the closer intelligence agencies work with investigators, the more likely it is that file searches will be sought.

There are several ways to reduce risk in this area. One is to limit the use of intelligence for law enforcement purposes. Another, assuming there is a compelling benefit in so doing, is to employ parallel investigatory efforts that keep intelligence out of the investigatory record. This is frequently done in customs cases and has been effective in the drug trafficking area. Another recommendation is to establish a "Center" that would focus on the use of intelligence in prosecutions. This Center might be staffed by Intelligence Community and Justice Department lawyers. The

Center would be the focal point for the Intelligence Community and law enforcement agencies once a decision has been made to use intelligence in pursuing the law enforcement action. Finally, the Justice Department is attempting to establish a protocol that governs when Intelligence Community files may or may not be searched. The Department wishes to limit searches to that intelligence used in developing cases. It does not appear that any statutory provisions to restrict discovery to protect intelligence sources are required at this time. There are concerns that legislation might be counterproductive, as such restrictions would likely to trigger greater interest in discovery actions and challenges by defense attorneys.

The intelligence and law enforcement communities agree that regardless of what standards are applied to permitting searches, the searches themselves must be conducted with maximum focus and coordination. By requiring prosecutors to closely define their search requests, the Intelligence Community may be able to conduct a timely and thorough search related to the specific framework of the search request. Specificity on the part of the request will help limit expectations that the Intelligence Community will search for every piece of information in all its files, which is burdensome and even unreasonable given the nature of much intelligence information collected.

Tasking

This issue pertains to whether and how law enforcement may "task" the Intelligence Community to collect intelligence related to a specific subject matter. As the intelligence and law enforcement communities have both become increasingly involved in the international aspects of weapons proliferation, terrorism, drug trafficking, international organized crime and the like, it is not surprising that law enforcement has been eager to consume the Intelligence Community's considerable wealth of information on these subjects. Much of this information is disseminated to law enforcement and other agencies as strategic intelligence. It has followed that in seeing these capabilities, law enforcement would at times like to task the intelligence community to collect on specific subjects. Of all the issues before the Interagency Task Force, this one has been the most difficult to resolve.

As it now stands, neither the National Security Agency (NSA) nor the CIA will accept tasking. Both organizations adhere to what is called the principal purpose test, which is that the main purpose of the collection is foreign intelligence. For its part, the CIA's Operations Directorate has agreed to a "tagging" procedure and will collect in response to a law enforcement request if the information has some foreign intelligence value. As long as the subject is a foreign person engaging in terrorism or weapons proliferation or other illegal activities, the principal purpose test is no problem. Problems arise when a foreign person of interest to the Intelligence Community enters the United States, or if there is an impending arrest and

prosecution. This is when problems arise relating to the protection of sources and methods in future court action, and when more rigorous analysis of law enforcement versus intelligence interests is required.

The JICLE task force has been meeting for months on the tasking issue and has concluded that both communities must steer away from tasking as much as possible. According to the report of the task force, "One way to minimize risks and ensure that case-specific collection is undertaken in a manner consistent with pertinent legal authorities is for law enforcement to provide target-specific lead information to Intelligence Community agencies. These agencies would determine if collection against that target would produce foreign intelligence. If the collection is done, the resulting information is to be disseminated to all interested consumers, as well as the law enforcement agency that provided the impetus for the collection." We believe this is the correct approach to take.

Training

The JICLE has recommended training for intelligence and law enforcement personnel to facilitate coordination and cooperation between the two cultures, and to educate participants on the laws, regulations and procedures that make the coordination process work. For example, Justice has been developing a training program for U.S. District Court judges on national security matters, to describe circumstances when it is permissible to disclose grand jury material to the Intelligence Community, and on the applicability of CIPA to all classified information, including the identity of intelligence agents. As the JICLE recommendations are accepted and incorporated as a way of doing business, training like this will be essential. It is unclear at this point how much the training will cost or how extensive the training should be. Most likely the greatest cost associated with training will be travel expenses for trainers and trainees. The cost should not be large; it is more a matter of competing for funds with other Department needs and objectives that may necessitate congressional interest in seeing that training will be carried out. JICLE believes that investigators and prosecutors, judges, intelligence officers, defense attorneys, congressional staffers and possibly the media would benefit from education programs. One proposal was to establish a Joint Law Enforcement/Intelligence Community Training Committee to assess training needs, evaluate training options, and prepare and deliver the training. Requests for additional funds for this training should be supported in the FY 97 authorizations of the intelligence and law enforcement communities.

Oversight Issues

One of the problems raised with regard to the closer nexus of intelligence and law enforcement is proper oversight of criminal investigations to ensure that criminal investigators do not adopt less stringent intelligence collection procedures in their

investigations, thus compromising the civil liberties of U.S. citizens. More specifically, there are concerns that criminal investigations might be pursued under Foreign Intelligence Surveillance Act (FISA) strictures, using bogus "intelligence requirements" as a subterfuge to avoid Fourth Amendment probable cause requirements.

There is some misunderstanding about the distinction between foreign counterintelligence (FCI) investigations and criminal investigations that has caused many to mistakenly believe one can readily supplant the other. It is true that FCI investigations may lead to a criminal prosecution, but FCI investigations are performed pursuant to Executive authority, as opposed to criminal statutes. Certain techniques are important to the successful resolution of an FCI case, including Foreign Intelligence Surveillance Court (FISC) authorized electronic surveillance and physical searches. The Truong-Humphrey case (4th Cir.) requires that FCI investigations maintain an intelligence focus. When the focus shifts from FCI to criminal, then investigators can no longer use FCI techniques. Evidence obtained through the use of FCI techniques after the focus shifts to criminal investigation would be suppressed. The use of criminal investigative techniques such as subpoenas and search warrants indicate that the investigation has a criminal focus. Therefore, investigators of FCI matters are denied the use of subpoenas, search warrants, grand jury testimony, and other traditional criminal investigative techniques.

The Justice Department does not see the relationship between these two kinds of investigations as a problem. The Office of Intelligence Policy Review (OIPR) and the Office of Legal Counsel work on intelligence gathering activities and authorities, and make legal rulings on matters such as the appropriateness of maintaining certain intelligence agents. The principal consumers of intelligence, on the other hand, are Justice Department entities such as the Drug Enforcement Agency and the Federal Bureau of Investigation, as well as the non-Justice agencies of the Treasury and Commerce. There is little overlap between the two groups in terms of common need. Moreover, the Attorney General is charged with overseeing both the monitors and the investigators.

In addition to the Justice Department overseers, oversight of FISA is considerable. FISA matters receive serious scrutiny by the FBI, OIPR and the Deputy Attorney General. FISA cases are the only Justice Department cases that are read by the Deputy Attorney General and Attorney General's staffs. Reports on FISA cases are also provided to the two Intelligence Committee.

There are two other oversight issues that were brought out by the JICLE pertaining to the provision of information to Congress. Sections 501 and 502 of the National Security Act of 1947, as amended, require the President and the DCI to keep the House and Senate Intelligence Committees "fully and currently informed of all intelligence activities . . . including any significant anticipated intelligence activity." There is no formal regulation that defines the circumstances when the Intelligence

Community may discuss ongoing criminal investigations with its oversight committees. The Law Enforcement Community has concerns that in meeting the statutory oversight requirements, the Intelligence Community will feel compelled to disclose information pertaining to law enforcement investigations. The JICLE has recommended that the Intelligence Community coordinate with the Law Enforcement Community before it briefs Congress on any subject matter with law enforcement implications. A December 1995 DCI Directive (DCID 2/13-1) confirms that the Justice Department will be informed before there is congressional notification on intelligence matters that have law enforcement information. The Directive establishes procedures to ensure advance coordination and resolution of disagreements between the intelligence and law enforcement communities on the amount of information that may be provided without adversely affecting a criminal investigation or prosecution.

Another recommendation from the Task Force's report is that the Intelligence Community should apply "substantially stricter standards before providing non-oversight committees with information on ongoing criminal investigations with significant intelligence implications."

Finally, the JICLE considered current procedures for disseminating clandestinely collected foreign intelligence that identifies congressional Members or staff. The current practice is that the identities of such individuals are removed before dissemination. However, any recipient of the information -- with the exception of the President, Vice President, Secretaries of State and Defense, and the National Security Advisor -- who wants to know the actual identity may be informed of that identity upon written request. The Justice Department has been concerned that this disclosure policy poses a threat to criminal investigative responsibilities and practices. When the JICLE met on this subject, several conclusions were reached. First, there is ample opportunity under the current procedures for the agencies that have collected this information to bring their concerns to the DCI before the information is provided to Congress. Second, due to concerns about interference with ongoing criminal investigations, the DCI or CIA General Counsel would obtain Justice Department permission before providing this information to Congress. If that permission were denied, the information will not be provided. There are some who believe these procedures should be reconsidered and that reporting to Congress should only be done when there is some foreign intelligence value to the information -- as opposed to domestic law enforcement or counterintelligence.

We may wish to consider this issue itself with regard to a need for clearer standards and procedures for the provision of this investigatory information to Congress. We, indeed Congress as a whole, should resist any recommendations that would further restrict it receipt of this kind of information.

Recommendations

Legislation

1. There is no need to further clarify the National Security Act of 1947, as amended, or the subsequent Executive Orders. There is a flexibility in these laws that permits a reasonable, but well-bounded, range of interpretation that will allow for improved cooperation and coordination between law enforcement and intelligence without blurring important demarcations between the missions and authorities of the two communities.

2. There has been debate over whether the Classified Information Protection Act (CIPA) should be amended. CIPA was enacted to provide a procedural mechanism for use in Federal criminal trials involving classified information. However, outside the Federal criminal process, there are no CIPA-like processes. Thus, some have suggested the creation of procedures similar to CIPA for use in civil matters. Those opposed to this approach believe it is unworkable and unnecessary, and would erode the viability of the state secrets privilege. Interagency review under the JICLE has concluded that there is no need for civil CIPA. Because of the complexity of this issue and the short legislative year this session, the Intelligence and Judiciary Committees may wish to study the CIPA expansion issue in the next Congress.

3. The Committee should consider statutory or other language that will set forth "reasonable" expectations and goals on Intelligence Community reporting on criminal activities. This language should convey Congressional views on the extent to which third party activities should be reported to law enforcement by the CIA and requirements pertaining to reporting on illegal actions by officers, employees, contractors or agents. The language should express legal requirements and set forth a national policy regarding the reporting of agent involvement in illegal activities, and the degree to which such activities should affect continued involvement with that agent. A balance must achieved between recognizing an agent's unsavory activities versus the value of intelligence the agent in question can provide and the validity of the requirement for intelligence that is driving the relationship between the Intelligence Community and the agent in the first place.

Resources

4. Training is essential to effective cooperation and coordination between the two communities. Consideration should be given to the need for additional funding for training in the FY 97 authorizations of the intelligence and law enforcement communities. This is an issue that should be worked with the State, Justice and Commerce Appropriations Subcommittee.

5. The Committee should continue to provide strong support to information management initiatives in the Intelligence Community.

6. Information management in the law enforcement community needs serious developmental planning and investment. Information management within the various law enforcement agencies is deficient; one result of this deficiency is poor information sharing among these agencies. The Intelligence Community, chiefly through its Centers, has built electronic data sharing links with the law enforcement community. The one exception to the link-up is the FBI, which has not participated due to the inadequacies of its ADP capabilities.

The Committee should encourage and support well-thought-out information management initiatives by the National Security Division of the FBI. Improvements here improve the work of the Division's International and Domestic Terrorism Sections. Information management upgrades for the FBI's Criminal Division, as well as other law enforcement agencies, are outside the Committees's oversight responsibilities. However, the Committee should discuss the importance of these needs with appropriations staff.

7. During the course of this study, the Committee became convinced that within the body of investigatory information obtained by law enforcement, there is important strategic information that is of value to others in the law enforcement or Intelligence Communities. Without better information management capabilities, at this time it is fruitless to require law enforcement to disseminate this information. However, plans for such dissemination should be a factor in planning for future information management systems.

Coordination

8. We feel it is unwise to pronounce categorically which agencies (intelligence or law enforcement) should or should not develop or have contact with human sources overseas. Applying a rigid directive to an area where there are an endless variety of cases and unique circumstances would probably do more harm than good. However, we believe that all anticipated and existing contacts with confidential informants, in areas where intelligence and law enforcement interests overlap, should be coordinated through the Chief of Station. The Chief of Station should be consulted prior to any effort of a law enforcement agency to engage in clandestine activities. Any unresolved problems should be resolved at the headquarters level of the parties involved in a disagreement.

9. Some have suggested that the FBI routinely act as the lead law enforcement agency for the purpose of coordinating law enforcement activities in a foreign country with the Ambassador. Because there may be other U.S. law enforcement entities in country that are not Justice Department organizations, designating the Justice Department as their representative, at least in a coordinating role, is too cumbersome and unrealistic.

10. There will be occasions when conflicts will arise overseas between law enforcement objectives and competing national security interests. We believe these problems can best be resolved if, from the outset, the Ambassador and the Chief of Station are kept reasonably informed of law enforcement objectives and plans so that all parties may weigh the implications of a law enforcement investigation or action in a particular country before it takes place. In cases where it is agreed that a law enforcement activity is not problematic or that these interests should granted primacy over other national security issues, similar interagency discussions in country also would serve to improve coordination and information sharing. In cases where differences arise that cannot be resolved in country, before investigations or other law enforcement activities are initiated, or State Department or intelligence activities are undertaken that it is believed could adversely affect a law enforcement action, We believe the conflict should be resolved at the highest necessary levels of government in Washington.

11. Some have argued that only U.S. law enforcement should conduct liaison with foreign law enforcement entities. We disagree with this premise, as set forth in a series of points made earlier in the body of this study. The CIA should be permitted to collect information from any foreign individual or entity deemed by the DCI or his designated representative to be of intelligence interest. Moreover, for the purposes of coordination, the Chief of Station should be kept fully advised of the law enforcement liaison activities of all law enforcement agencies in country where intelligence and law enforcement interests overlap. This level of coordination should in no way require the unauthorized disclosure to the Chief of Station of restricted law enforcement investigatory information or cede to the Chief of Station any prosecutorial authority.

INTELLIGENCE COMMUNICATIONS

Executive Summary

Since Operation DESERT STORM, there have been increasing calls for improved and more timely delivery of information products from the intelligence producers to the end users. Communications has often been described as the critical need to, and problem in, "moving" information in a timely fashion. Because a significant amount of Intelligence Community (IC) funding goes into the delivery of products, the Committee, as part of the *IC21* process, reviewed the IC's role in providing communications as part of its task to disseminate relevant information to its customer audience. Critical to this review was the Committee's narrowly defined differences between "communications," the focus of the paper, and "dissemination." Specifically we defined "communications" as the conduit(s) for moving data from one point to another. This includes the standards necessary to interface hardware and software to the communications conduits. Alternately, the term 'dissemination' is defined in this paper as the process of moving data from one place to another. It includes the functions of providing information content, formatting it, securing it, transmitting it (in whatever form), and when necessary interpreting it at the receiving end. Within these definitional boundaries, the study's conclusions provide three main themes.

First, the IC is fully responsible for timely dissemination of its products. However, the IC should not be responsible, as a core competency, for developing, procuring, managing or maintaining the communications required for those dissemination functions. These are core competencies for the communications communities such as the Defense Information Systems Agency (DISA), and Diplomatic Telecommunications Service Program Office (DTSPO) and others. Further, the concept of Command, Control, Communications, Computers and Intelligence (C4I), which was a contributing force for the IC to be involved with providing communications is an artificial construct that does not provide a true integrating force.

Second, the IC should retain some minimal number of communications professionals to provide the necessary technical interfaces and requirements to the communications community and to provide those communications needs, esoteric to the IC, not provided by the professional communicators.

Finally, there is a need for a thorough review of the IC's communications requirements to determine current and future needs. Within the construct of such a review, the IC needs to fully ensure its equipment can properly interface with the various provided communications media. To do this, the IC's equipment must be fully compliant with current and emerging communications standards and protocols. This also includes the need for the IC to ensure its products are available to the end customers in both the form and format necessary for the specific user.

The full study goes into detail on each of the above themes.

INTELLIGENCE COMMUNICATIONS

Study Purpose

Ever since Operation DESERT STORM there have been increasing calls for improved and more timely delivery of products (particularly of imagery products) from the intelligence producers to the information users. Communications (in the form of "bandwidth") or the lack thereof has often been described as the critical need to, and problem in, "moving" information (in its various forms) to the users in a timely fashion. During the fiscal year 1996 budget build, the Committee placed a good deal of emphasis (and money) on the "downstream" processing and dissemination of intelligence. Because a significant amount of Intelligence Community (IC) funding goes into the delivery of products, this study focused on reviewing the IC's efforts to disseminate its information. Specifically this paper attempted to identify, and make necessary recommendations for, the IC communications infrastructure, architectures, systems and capabilities/capacities needed for the 21st century.

The IC funds numerous communications media for the delivery of information to and among producers and users. These communications media include both the "bandwidth" (or communications pipes -- whether they are radio links, satellite communications, or telephone lines) and the equipment (radios, terminals, encryption devices, etc.) for processing the information at both the transmitting and receiving ends. Our goal was to determine if the current and projected communications efforts are logical for the 21st century.

Study Approach

It should be first noted that this is not a scientific study, but rather an assessment of intelligence communications management and structures based on Community expert inputs. At the outset of the study, it quickly became obvious that an in-depth level of detail was not achievable in the time allotted, or even logical for a study of the IC. Additionally, the team had no intention to attempt to predict specific communications spectra, bandwidths, data throughputs, etc. Such analysis was beyond the scope of this effort and would have been merely guesses for needs 10 to 15 years into the future. The team interviewed experts and leaders from both the intelligence and communications communities. This study, more than any other *IC21* study, was limited in scope and nature -- and nearly terminated as formal study -- specifically by the fact that the IC does not "own" communications ("pipes") or any specific portions of the RF spectrum, nor is the function of communications a core mission for the IC. The IC requires the support of the communications community, and is actually better defined as a customer of communications. After an adjustment of the original goal, the study did attempt to qualify this external support and provide recommendations for any improvements. For the purposes of this report, we have

generally aggregated the Defense Information Systems Agency (DISA), the Joint Staff J6, the Diplomatic Telecommunications Service Program Office (DTSPO), the Military Communications and Electronics Board, the service and agency communications directorates, and so forth, under the rubric of "communications community" (CC).

Also, it is important to acknowledge a difference between "communications," the focus of this paper, and "dissemination." In the context of this paper, "communications" is defined narrowly as the conduit(s) for moving data (regardless of data type) from one point to another. This definition includes the standards necessary to interface hardware and software at either end of the communication conduit. Alternately, the term "dissemination" is defined in this paper as the entire process of moving data from one place to another. It includes the process of providing the information content, formatting it, securing it, transmitting it (in whatever form), and when necessary interpreting it at the receiving end. These definition explanations are important in understanding the thrusts of this paper.

General Conclusions

A. The IC is responsible to its customers for timely dissemination of its information products in the required forms and formats. However, the communications needed to disseminate these products are not, and should not be, a core competency for the IC. This core competency is more justifiably a function for the CC. Within this context, the CC should be the "provider" of the IC's communications and communication infrastructures and the IC should, as the "customer," state specific and well-defined communications requirements. Despite this general position, some intelligence operations, particularly clandestine/covert, will continue to require some unique organic IC communications capabilities.

B. The concept of Command, Control, Communications, Computers, and Intelligence (C4I) is a construct that, ostensibly, integrates operations, intelligence and communications into a cohesive and seamless entity. The concept was developed to reduce the we (intelligence) and they (operations) mindsets that hampered true integration of operations and intelligence. However, C4I is more of an artificial construct that "makes for good press," than a true integrating force. Additionally, the current and foreseeable organizational structures and procedures do not provide for true C4I. Regardless, C4I is a good concept for moving to an integrated future and it will be more relevant in tomorrow's integrated (military) ops/intel and communications environment.

C. Timely delivery of intelligence products to users in the proper form is a general IC weakness. The Community historically has developed, or added, intelligence product delivery (including communications systems) as an afterthought in the development of intelligence capabilities. The IC could benefit from a more integrated communications architecture and process which is thoroughly

considered, designed and developed at the outset of an intelligence system's (and operational user's system's) development. Additionally, data throughput (usually equated to bandwidth) is typically not adequate.

D. The IC funds numerous communications systems and associated equipments. Some of this practice should continue. However, in this context, the IC must become the communications "retailer" and the communications community must become the "wholesaler." That is, the CC must be involved at the outset with, and have coordination authority over, such developments and operations. It should provide specific standards and interface protocols to which IC systems should be designed. While the CC should be the communications path provider, the IC should continue to develop/purchase its required terminals/end systems. Additionally, for those unique and specialized communications requirements, such as for covert operations, the IC should continue to fund/provide for the necessary capabilities.

Specific Conclusions/*Findings* (It should be noted up front that several of the findings and associated recommendations below have some overlap. This was specifically done to ensure that nuance differences between related issues was not lost.)

A. The IC is responsible to its customers for timely dissemination of its information products in the required forms and formats. However, the communications needed to disseminate these products are not, and should not be, a core competency for the IC. This core competency is more justifiably a function for the CC. Within this context, the CC should be the "provider" of the IC's communications and communication infrastructures and the IC should, as the "customer," state specific and well-defined communications requirements. Despite this general position, some intelligence operations, particularly clandestine/covert, will continue to require some unique organic IC communications capabilities.

1) Modern, sophisticated communications technologies are generally evolving more rapidly than IC systems and associated communications infrastructures can maintain pace.[1] In fact, one respondent remarked that "it is too difficult for any (non-communications professional) organization or system to stay on top of these technology changes." However, the IC, today, employs communications experts to satisfy many, and arguably most, of the IC needs. Although these experts provide an invaluable service to the Community, it is the *CC professionals* working the communications needs for the operational, intelligence, logistics, maintenance, and other communities who have a better "finger on the pulse" of current and evolving technologies. They are *in a better*

[1] Various sources, including: commercial industry papers, personal interviews, and communications seminars.

position to make the necessary decisions for ensuring proper communications are available to all users. They are also in the best position to provide the "integration layer" (the technical buffer, if you will) between the rapidly evolving communications media and the end users.

2) *The technical focus of all modern communications needs is driving toward commercial solutions and equipment.* The U.S. Government (USG) is no longer in the position, nor does it need, to provide the majority of the communications paths for its command and control and support (including intelligence) needs. With the exception of satellite communications, the USG is behind or rapidly falling behind the commercial market in terms of being able to provide cost effective, robust, and flexible (flexible bandwidth on-demand, for example) communications. *Therefore, proper leveraging of the commercial market provides the greatest potential for ensured, cost-effective communications support.* Such leverage will only be possible by aggregating communications needs and having a professional organization (or organizations) negotiating with the commercial carriers for the bulk "bandwidth," "pipes" and, increasingly, the communications services themselves. The latter will be true as communications providers will increasingly be able to provide communication network services as well as the communications circuits to meet government requirements.

3) A few words on the Diplomatic Telecommunications Service Program Office (DTSPO) can illustrate the thrust of these arguments. DTSPO is a centralized communications organization. Over 40 agencies (including the IC) have their requirements aggregated and satisfied by DTSPO. DTSPO's approach allows for the use of a single communications "pipe," commercially provided, into an embassy. Because DTSPO aggregates the requirements, it can acquire the necessary bandwidth competitively. And, since the commercial providers have a financial incentive to be the most effective (both in terms of cost and capability) provider "on the block," DTSPO can negotiate the best product for cost. Additionally, as the commercial technologies change, DTSPO can go to the commercial providers to recompete the requirements. Again, financial incentives motivate the commercial providers to provide the best possible service. *Under this approach, DTSPO can design and optimize the necessary infrastructure(s) to handle all requirements -- voice, data, secure voice/data, etc. Since the group of requirements is consolidated, there is no need for separate communications infrastructures to satisfy the needs.*

4) Because of the commercial industry leaps in capabilities, the future government communications planner, particularly IC communicators, will become less the providers of communications, and more the experts who understand the commercial providers and know how to best employ/exploit these commercial capabilities. Again, *the best use of USG resources will be to*

ensure proper aggregation of communications requirements such that a consolidated need, or set of needs, can be provided to commercial suppliers for negotiation. With this in mind, (and as stated above) there appears to be a good deal of logic to consolidate the communications experts into the CC. Regardless, very likely the most important IC communications function will be to ensure the development of proper, logical, considered, and technically specific statement of requirements. Such requirements should be provided to the CC that, in turn, goes to the commercial providers to satisfy the needs based on the CC's architectural and standards-based constructs.

5) Standards, then, would be the next logic discussion point. Currently, the Defense Information Systems Agency (DISA) is developing the standards, and procuring the communications "backbone" (both media and bandwidth) for the Global Command and Control System (GCCS) and the Defense Information Switched Network (DISN). A brief definition of DISN is:

> "DISN is the DoD's consolidated worldwide enterprise-level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations. It is transparent to its users, facilitates the management of information resources, and is responsive to national security and defense needs under all conditions in the most efficient manner."[2]

This communications infrastructure (which depends on both commercial and government carriers) will provide sophisticated, flexible (on demand), and robust communications for all of DoD (and other) agencies. This architecture (which is also designed to inhibit offensive information attack) should be the infrastructure of choice (or of mandate) used by the IC. Again, the IC should allow DISA (as part of CC) to become the standardized, and standards'-based "communications provider." The IC needs to focus on its core competencies, and more simply be a communications user with specifically identified requirements.

6) As has been stated, *DISA is tasked with, and has to ability to procure the best available communications media for the best price.* This includes owning organic systems (Defense Satellite Communications System (DSCS) for example), managing/directing use of tactical radio communications, and leasing commercial landlines or other government systems. Also as stated before, the IC does a fair job of satisfying some of its it own communications needs, however, it is not as well suited/versed as is DISA in this area. Therefore, some of the most important future challenges will be the IC's ability to state

---

[2] Definition approved by ASD (C3I).

clear requirements to DISA for, and DISA's management ability to provide/allocate, the necessary communications paths/bandwidths for the total USG requirement while minimizing costs.

7) The individual components of the IC have done a fair, to good, job in projecting their stovepiped communications needs. The National Reconnaissance Office (NRO), for example, has done a good job of identifying its communications capacity needs to the year 2000 and beyond. However, *the IC has not done a thorough aggregated study of its entire future communications needs*. Such a study needs to be accomplished and provided to the CC to allow it to provide a cost-efficient, total solution.

Findings/**Recommendations**

8) **The IC should focus on its core competencies of intelligence collection and processing. DISA, and like organizations, should be the "communications providers" who move the resulting information. The IC should, quite, simply be a user with specifically identified requirements.** *Such a construct may provide less flexibility, but has the potential for better, and more effectively, fulfilling the totality of USG communications needs of the future.* This recommendation fully considers the fact that the IC is responsible for dissemination of its products to the identified customers. However, the recommendation focuses on the position that the IC should not be in the "communications business."

9) **The IC should request all communications support (for "bandwidth") through the CC. Before such a request (or better stated, continuing requests) can be made, a thorough study of total IC current and future requirements will have to be accomplished. Such a study should be the responsibility of the Deputy Director of Central Intelligence for Community Management (DDCI/CM) (the concept contained in the *IC21 Intelligence Community Management* staff study). Additionally, it will have to be kept up-to-date through continuous review as new capabilities and technologies are brought into service.** It should be noted that in order to make such a proposal work, there will be a corresponding increase in the responsibilities and, therefore, personnel requirements on the CC. A to-be-determined number of IC communications professionals will most likely have to be reassigned to organizations such as DISA and DTSPO.

10) **The DDCI/CM's Intelligence Support Office (the ISO is a construct identified in the *Intelligence Community Management* staff study) should maintain a consolidated core of communications professionals whose primary tasks will be to act as the "technological knowledge bridge" between the (CC) providers and the (IC) users, to define communications (and dissemination)**

standards for the Community, and review current capabilities and develop migration plans to meet developed architectures and standards. This will require that IC communications professionals be sufficiently technically proficient in IC terminals, computers, systems, etc., as well as with the communications "pipes" and providers to be able to logically identify specific requirements and ensure the CC provides the necessary "bandwidths." **Additionally, the ISO's organic communications experts need to develop or procure the critical "specialized" communications requirements/services for those <u>few</u> users not specifically provided for by the CC.** This would include the specialized needs of direct down-link systems, specific data relay systems, collection system unique data links (such as the common data link from the U-2 and others), covert communications, etc. However **these should be the exception rather than the rule.** In order to coherently make this recommendation a reality **there is a need to consolidate the IC's communications professionals into a Community-wide Infrastructure Support Office.** This would require that all agencies and services communications professionals be assigned within this single organization (presumably, then, with a single reporting chain and boss). Such a consolidation will be painful and (likely) bitterly opposed. However, it would provide better Community-wide communications continuity, most likely a reduced force structure need, and would dove-tail nicely into recommendations being discussed in the *Intelligence Community Management* staff study.

B. The concept of Command, Control, Communications, Computers, and Intelligence (C4I) is a construct that, ostensibly, integrates operations, intelligence and communications into a cohesive and seamless entity. The concept was developed to reduce the we (intelligence) and they (operations) mindsets that hampered true integration of operations and intelligence. However, C4I is more of an artificial construct that "makes for good press," than a true integrating force. Additionally, the current and foreseeable organizational structures and procedures do not provide for true C4I. Regardless, C4I is a good concept for moving to an integrated future and it will be more relevant in tomorrow's integrated (military) ops/intel and communications environment.

1) The basic concept of C4I considers communications, computers and intelligence as fully integrated into, and coordinated <u>with</u>, command and control of operations. However, most respondents believe today's C4I construct is mainly focused on communications and intelligence support <u>to</u> operations, rather than "achieving the goal of integrating communications into all operational enterprises such that mission people can focus on the mission and the infrastructure people can focus on the infrastructure."[3] *Today's*

---

[3] Personal interviews with IC and CC experts

constructs of ASD (C3I) (separate from operations for example) and the services' Napoleonic organizational structures of J2 (intelligence), J3 (operations), and J6 (communications) does not well foster this concept. Therefore, there is a valid argument that can be made that C4I is simply a well-intentioned term rather than reality.

2) There is a C4I document that states that the concept of the C4I "infosphere contains the total combination of information sources, fusion centers, and distribution systems that represent the C4I resources a warfighter needs to pursue his operational objective."[4] The thrust of this concept is that all available information, regardless of source (including the IC) must be virtually available any time any where to any user (user not being defined). In today's organization and systemic structures, "C4I systems" are typically designed and developed to follow the specific "chain of command." Often, this chain of command does not include all specific (or varied) end users of information provided by disparate sources. For example, there is little to no ability to get imagery from a UAV directly to a soldier in a foxhole even though this may be technologically feasible. Often these "chains of command" specifically deny information because of the "knowledge is power" paradigm (commanders do not always want or need uninhibited "total knowledge" at all echelons). This effectively denies, or at best, inhibits the true concept of C4I. Additional barriers, more esoteric to the IC, also need to be overcome. These include intelligence data (e.g., source identification) policies and security. Specifically, the IC needs to take a fresh look at intelligence data to see what can logically and safely be downgraded to unclassified (or at a minimum, collateral SECRET) levels. Today's "infosphere" requirements -- that is information dissemination requirements -- can be satisfied, but only by digital communications systems developed with, and focused on, recognized standards that allow for the totality of integrated operations/intelligence/maintenance/logistics/etc. *The IC needs to ensure any communications systems it develops or uses conforms to the user standards and are available to any user at any level and at any necessary security classification level.*

3) *The concept of "C4I for the warrior" is not well considered when discussing CIA support to military operations.* CIA support to the "national collection requirements" needs to remain separate from the military concept of C4I, but not from the concept, where possible, of standardized structures that provide integrated operations, intelligence, logistics/maintenance, and communications to users (again, at any level and classification).

---

[4] USSOCOM C4I Strategy into the 21st Century.

4) It should be noted that intelligence support within the concept of C4I is becoming more a part of the operational users' everyday thinking. However, this needs to be further improved. LtGen Minihan, Director, DIA, has stated that the IC of the 21st century will be a warfighting participant, not a warfighting support agent. This concept of participation (vice support) is critical, for *if this does not become a norm, the concept of C4I will fail to fulfill its potential.* Simply stated, intelligence must become a warfighting weapon employed by the user just as is a radar or a gunsight.

5) As a further thought on the concept of C4I, but more specifically focused on the support to military operations mission, *intelligence operations of the future must be thoroughly integrated into the users' operational and support mechanisms (read: hardware systems) to ensure viability and utility.* Logically, the future SMO communications environment will be completely seamless (and transparent to the user) with C2 and intelligence communications riding on the same hardware (user terminals and transceivers) with multi-level security systems. Intelligence systems will have to be integrated with these operational systems as *the tactical consumer should not have to tolerate supporting multiple, stand-alone pieces of equipment.*

6) There is one additional commentary on IC communications supporting operational users. *Far too often, intelligence support communications are "cobbled together" to satisfy operational requirements for a given location or contingency.* (The current communications architecture being developed for Bosnia is a case in point.) This is true since much of the IC's communications support/architecture is designed for in-garrison use and there is usually little to no preplanning for the communications architectures of specific (contingency) locations. *This is partly due to insufficient planning and exercise done within the IC to develop or practice with contingency communications systems, architectures, and links. It is also largely in part due to the fact that the IC can not possibly prepare for every unknown situation.* However, there is still a need for the IC to exercise its communications systems, particularly those in the theaters outside the continental United States, regularly to validate their architectures and designs, and to ensure that stated user requirements, in the continuum from peace through war, can be met.

Findings/**Recommendations**

7) **"Intelligence communications" must be better designed to provide "deployed" support as well as "in-garrison" support. Such support must be transparent to the user during deployments to the operational theater.** This requires a "virtual communications infrastructure" that is either independent of location (i.e., not bound by physical connections) or provided with (and trained on) adequate physical communications media for world-wide deployments. **Use**

of such capabilities need to be regularly exercised to ensure viability and capability.

8) **Based on specific requirements, communications support to intelligence dissemination must be fluidly and transparently available from the highest (national) to the lowest possible user/tactical level.** This should include the ability to (simultaneously if needed) provide intelligence information to any/all user levels. As to this issue, the IC needs to address dissemination-specific issues such as data simultaneity (availability of a piece of information at multiple levels at the same time), data fusion and tailored products (right information, in the right format, at the right time). *This is less a technical communications capability limitation than it is an operational intelligence dissemination mindset limitation.* A case in point was the 1995 PREDATOR UAV deployment in support of operations in Bosnia. The dissemination technology involved easily allowed for the air vehicle's imagery to be provided to the Secretary of Defense (SecDef) and the Director of Central Intelligence (DCI) as well as to the intelligence officers at Aviano Air Base (or even a reconnaissance platoon -- had there been such on the ground in Bosnia) simultaneously. However, such simultaneity is not typically realized. Two issues must be resolved to make this possible. **First, the IC must work directly with, not apart from, the operations, communications and development communities to ensure that required dissemination of IC data is considered at the outset of system development and/or employment. Second, there is a critical need to "bring operational thinking up to" the modern-day age of available technologies. This is, users must fully understand, appreciate, and allow for the possibilities -- not just the drawbacks -- of having information available to all participants and users simultaneously.** There is, in fact, a tendency by both the intelligence and operational communities to limit dissemination for fear of the use of the "seven thousand mile long screwdriver" (e.g., the ability of decision-makers, "inside the Beltway," to have over-the-shoulder look at, and often second guessing of, operational commanders).

9) **As briefly stated above, the IC must focus more effort on integrating intelligence systems (or, more justifiably, the display of intelligence data/products) into users' operational systems.** It is not only critically important to minimize the number of stand alone systems the operators must learn, use and maintain, but it is technically possible to integrate such capabilities as the standards for hardware and software become better defined and refined. The IC should take advantage, to the extent possible, of the users' equipment already fielded rather than providing more "boxes" (this is not to say that there will not be some need for unique stand-alone systems to ensure needed capabilities). **However, to the extent possible, the tactical user must not be forced to operate multiple, stand-alone pieces of equipment.**

10) In order to ensure that the necessary communications support for the dissemination of intelligence products is continuously available (particularly for contingency operations), **IC communications requirements must be well thought out and capabilities planned prior to any operation. Additionally, to ensure the compatibly of intelligence systems with supporting communications systems, the IC needs to specifically identify (or be provided) all interoperability requirements at the outset of an intelligence system's development.**

11) **The Office of the Department of Defense should reassess the current organizational structure of Assistant Secretary of Defense (Command, Control, Communications and Intelligence).** This organization is based on the concept of integrating communications and intelligence which, as stated above, is a logical operational imperative. However, also as stated above, intelligence is a unique (not communications) function that relies on communications support, just as does the operations, logistics and maintenance functions. The ASD(C3I) organizational structure supports this argument by disassociating the intelligence and communications functions into two separate Deputy Assistant Secretaries -- one for Intelligence and Security and one for Communications. DoD should relook this organizational structure to more logically and appropriately focus intelligence functional core competencies and the communications support core competencies.

C. Timely delivery of intelligence products to users in the proper form is a general IC weakness. The Community historically has developed, or added, intelligence product delivery (including communications systems) as an afterthought in the development of intelligence capabilities. The IC could benefit from a more integrated communications architecture and process which is thoroughly considered, designed and developed at the outset of an intelligence system's (and operational user's system's) development. Additionally, data throughput (usually equated to bandwidth) is typically not adequate.

1) Although the IC suffers from several communications delivery shortfalls, two primary issues boil down to limited bandwidth and system incompatibility. The first of these is typically result from the development and use of *stovepiped systems designed for single purposes (i.e., movement of imagery).* Communications bandwidth is expensive. And when communications are developed or purchased for stand-alone capabilities, typically they are (minimally) sized for the specific, single purpose. This can result in inefficient use of the bandwidth (the communications media are not used full time), and the need to buy duplicative communications (for the other stand-alone capabilities). Also, as stated above, *the IC's communications systems are often not compatible (particularly in terms of security devices) with the users' communications systems.* Far too often the IC employs systems with security devices designed for classification levels higher than what the users can, or

want to, employ. This forces system incompatibility, and therefore the need for additional equipment (to translate one for the other).

2) *Because of their more limited flexibility (access to multiple communications paths), the IC's "stovepiped" communications systems may be more susceptible to Information Warfare (IW) attacks than is the more flexible DISN system of systems.* This is not to say that DISN is not susceptible to such attacks, but it is to say that a coordinated, centrally-managed communications architecture may provide more robust flexibility, and therefore, survivability, than what the more stand-alone IC systems can provide today. It should also be noted, that some respondents stated the IC's systems may be less vulnerable to such attacks because of their increased security. This may be true, but, again, the robustness (communications path flexibility) must be a consideration in such discussions.

3) *The IC's communications capabilities have often been too highly classified for users to receive directly.* This has forced analysis or fusion centers to review and selectively downgrade information before it can be provided to users. Fortunately, systems such as the Tactical Information Broadcast Service (TIBS) provide automatic security downgrading such that the information can be provided directly from the producers to the tactical (and other) consumers. *This sort of automatic downgrading needs to be expanded where possible.* Additionally, *there is a need to review security practices at all levels to determine downgrade potentials of any/all data.* As stated before, a goal should be that no IC data provided to the user is classified higher than collateral SECRET.

4) A finally word on DISA. In addition to the DISN, DISA has also developed the Defense Messaging System (DMS). DMS will provide the Community with standardized message handling. This program, and particularly its cryptographic components, have the potential to greatly increase the ability of the IC (and others) to use common platforms (user terminals, etc.) and common communications infrastructures while maintaining (electronic) separation for security purposes.

Findings/**Recommendations**

5) **The IC should not maintain separate communications systems (the communications media or hardware), particularly after DISN is fully implemented. The IC should specifically and thoroughly state data rate and capacity requirements to the applicable providers and user within the CC.** The communities (user, intelligence, and communications) should then decide on the standardized formats, hardware, etc, to ensure logical, coordinated, and seamless communications can occur.

6) **To ensure required data movement, the IC should be fully compliant with the emerging standards of the GCCS and the DISN whenever and wherever possible.** Compliance should not be selective. However, *there may be specific and unique requirements of the clandestine or special forces operations, for example, that must be considered and satisfied*. These, may not be satisfied by the standardized communications structures and capabilities.

7) **Although more a function of the dissemination process rather than specifically communications, the IC should review security practices for current applicability.** The IC has historically (at least from the users' perspectives) remained behind the "green door" of security. This has allowed, and in fact at times, forced the IC to take separate paths (apart from the user community) relative to communications. This cannot be allowed to continue. The IC needs to review its security practices to ensure that only those elements which need protecting are, in fact, protected, while providing the user the most amount of useful data possible and necessary. Often, for example, the IC needs only to highly protect the source of information, but not so much so the information itself. The IC needs to relook its security requirements to ensure only that which needs protecting, is. This should include a review of what data elements can be automatically downgraded via machine such that the sources of the data can not be discerned.

D. The IC funds numerous communications systems and associated equipments. Some of this practice should continue. However, in this context, the IC must become the communications "retailer" and the communications community must become the "wholesaler." That is, the CC must be involved at the outset with, and have coordination authority over, such developments and operations. It should provide specific standards and interface protocols to which IC systems should be designed. While the CC should be the communications path provider, the IC should continue to develop/purchase its required terminals/end systems. Additionally, for those unique and specialized communications requirements, such as for covert operations, the IC should continue to fund/provide for the necessary capabilities.

1) The IC "owns" a number of its own communications systems and, in fact, communications "pipes" such as CRITICOM, TIBS, DSSCS, etc. However, *these communications pipes were developed to satisfy specific IC needs that could not or were not satisfied by the communications infrastructure of the past*. Although some of these systems "ride" on communications paths provided by the communications community, they do not necessarily conform to the communications infrastructures/standards of today's modern capabilities. *Such systems could be amalgamated under the centralized organization of the DISN*. This would ensure compatibility is a USG-wide reality.

2) In the past, the IC developed and "owned" a number of unique communications capabilities primarily based on the needs for specific/unique data throughput rates (imagery, for example), high security, and assured receipt of data. However, in the future, *the IC should not be in the business of providing stand alone, unique or organic communications systems, infrastructures or communications "pipes."* The extraordinarily rapid evolution of communications standards, capabilities, capacities, flexibility and security obviate, and in fact, mandate, the IC to be a subscriber to the larger communications community.

3) *To ensure timely delivery of intelligence information to users, the use of broadcast technologies (such as TIBS) needs to be continued and improved.* The ASD (C3I) has recently approved the "Integrated Broadcast Service (IBS) Plan." This plan provides for the integration of the Tactical Information Broadcast Service (TIBS), the Tactical Related Applications (TRAP) Data Dissemination System (TDDS), the Tactical Reconnaissance Intelligence eXchange System (TRIXS), TADIXS-B, and the BINOCULAR efforts into a standardized protocols with compatible hardware and software. This effort was directed by the 1996 House Intelligence Bill, and needs to be fully supported by Congress in the future.

4) The IC funds for a number of tactical information dissemination systems (the "end terminals" on IC funded platforms) that conform to established CC standards. These include JTIDS, TADIL-A, TADIL-B, etc. compliant radios, terminals, etc. Although such systems are not the primary focus of this paper, funding for employment and use of these systems will need to continue. Additionally, the IC funds for unique collection data links, including the Common Data Link (CDL) for use by the U-2 and its ground stations, the RC-12 and its ground stations, etc. Because these links are integral parts of the collection systems, and not expressly designed for end product dissemination, this funding support will need to continue as a function of the IC.

5) The CC is focusing some efforts into the development/exploitation of direct broadcast service (DBS)/global broadcast service (GBS) technology developed by the commercial industry. Such services have the potential for very high bandwidth and data rates necessary for IC needs. The IC is reviewing the possible applications of this technology to move large amounts of data around the world, and should continue to play a positive role (including funding where necessary) in these efforts.

6) *For those systems and communications paths the IC must procure, commercial-off-the-shelf (COTS) products and commercial communications paths must become the normal acquisition goal.*

7) The IC buys and pays for some communications bandwidth on various satellites, land lines, etc. However, as stated previously, *the CC is in the best position to negotiate for the necessary bandwidth for the best price*. By allowing the CC to provide the IC with the necessary capabilities, the CC will inherently have the flexibility in bandwidth allocation/procurement that will allows it to provide the best possible support to a wide range of customers. This must be the bottom line goal.

8) Modern cryptography is evolving to a point where forced human intervention is becoming obsolete. Earlier systems typically required a communications center (with associated personnel) to encrypt and send, and receive and decrypt classified materials. Often the IC requirements for this sort of operation included having IC employees (rather than CC employees) handle the materials throughout the process. However, this need to draft a message, send it to an individual to have it encoded, then send the coded message to the communications center is giving way to automated message preparation, encryption, and transmission -- from an individual's desktop. *An IC goal for this type of technology should be to put encryption/decryption as close to the user as possible*. This will have a direct and positive effect on the IC specifically with respect to those operations where IC communications personnel had to be employed, often along-side (and often in duplication) of their CC counterparts.

Findings/**Recommendations**

9) **The IC should not directly contract for communications "bandwidth." Rather, communications requirements for bandwidth or satellite time, etc. should be provided to, DISA, for example, and funded in the standardized Service/Agency budget line items.** The IC should determine its yearly (or more) requirements, state these in terms of time, data throughput, timeliness, format (in some cases), and location (where is information needs to be). These requirements are then the responsibility of the CC to satisfy. This concept may require the IC to budget and provide funding to the CC for its communications services. The study does not recommend the CC budget for the IC's communications requirements.

10) **The IC should only budget and pay for those unique communications hardware and software capabilities necessary for IC systems to develop and "ship" their data/information, receive others data/information or for which such unique requirements exist (e.g., clandestine communications) that would preclude the CC from satisfying requirements.** This would mean that the IC would pay for the ability of its systems to collection, analyze, prepare, and ship to a communications point for dissemination. It also would mean that the IC pays for radios, transmitters, etc. necessary as part of an overall weapon system's (i.e., a UAV, a field site, or a reconnaissance aircraft) development.

11) **The IC, through the CC and user communities, should vigorously pursue advanced broadcast technologies including, IBS and GBS, to satisfy dissemination requirements.**

12) **Despite the recommendations for the CC to be the communications provider, and the IC to be the "user," the IC must retain a sufficient number of organic communications experts to provide analysis for stating requirements and for developing the required architectures. This includes those experts necessary to ensure the organic communications for those few unique efforts better left to the IC. Additionally, these experts should be integrated from the various services and agencies into a centralized IC infrastructure organization.** This will provide the necessary capabilities, while reducing the disparate support organizations within the various services and agencies. While it may be true that the *(to-be-determined) number of communications experts within the IC can probably be reduced as the CC assumes the IC's communications responsibilities, these same resource (people) may well be required within the CC to ensure proper requirements satisfaction.* **This recommendation requires significant additional and careful study.**

13) **Finally, for those systems and communications paths the IC must procure, and in some cases, own; commercial off-the-shelf (COTS) systems and, if possible, communications paths must become the normal acquisition goal.** Accomplishment of this goal will serve two primary functions. First, the cost of the equipment (particularly within the developmental side) will decrease. And, second, the standards-based commercial systems will allow the IC to better coordinate and integrate its systems and programs in with those of the user and communications communities.

Conclusions

A. The very obvious thrust of this assessment is to get the IC out of the communications business. This is not to say the IC cannot be a builder, but it is to say the IC should not be the architect. As the IC "backs away" from organically satisfying its own communications requirements, two specific paradigm shifts will have to occur. First, the trust factor between the IC and the CC will have to improve. That is, the IC will have to understand, and believe, that its requirements are not, generally, so unique, that they can not be satisfied by the communicators. Secondly, **the IC will have to be held accountable for identifying its real communications needs, and the CC will have to be held accountable for satisfying those requirements.** Communications cannot be taken for granted. They are the basis for making information available to the right user, at the right time. However, the IC should focus not on those issues, but rather on the core mission of ensuring the proper collection, evaluation, production and presentation of information.

B. All of the above observations and recommendations (even if adopted) do not ensure communication. That is, we can build compatible communications infrastructures and still not be able to move information because of the ways we display, store, or intend to make knowledge of that information. Specifically, we can, and do, have data bases that are not accessible due to their unique designs, or message/display formats that are not comprehensible to the intended user. Therefore, it needs to be understood that the standards discussion provided above are for the communications paths and pipes themselves. Remembering that communication only occurs when an intended message is sent, is received by the intended recipient, and the intentions are understood. Therefore, it must be understood that the discussions above extend only to the communications means, not to the "message" conveyed through those means. This later subject could easily be the issue of another (full length) study.

CONGRESSIONAL OVERSIGHT

Executive Summary

Findings

- The current intelligence oversight system arose from a view that intelligence had to be handled in a manner that was extraordinary when compared to other functions of government. Although that view may have been warranted in the aftermath of the investigations in 1975-76, it is not warranted any longer. Indeed, by continuing to view intelligence in this manner, oversight and the work of the Intelligence Community are likely made more difficult.

- Advocacy for overseen agencies is legitimate and to some extent necessary. This has not been an accepted stance for the intelligence committees. We agree with the view of former DCIs that intelligence is such a restricted issue that Congress must be more active in building the necessary political consensus.

- The current oversight system has been largely effective, and clearly has responded to those problems that prompted the creation of the current committees.

- There is no compelling reason to convert the current system to a joint committee. Congress's record regarding safeguarding highly classified information is not perfect, but does not warrant this step. Creating a joint committee would also require either the House or the Senate to alter its current arrangements for intelligence oversight, which has not had significant support in the past. Finally, and most importantly, creating a joint committee for intelligence would continue to heighten the view that intelligence is something other than an accepted function of government, which tends to increase rather than complement oversight issues and problems.

- Although the reasons for which the current committee was made a select committee with tenure limits may have been valid in 1977, these may no longer be compelling or valid. There are equally compelling arguments in terms of the general effect of these arrangements on oversight to warrant reconsidering them.

- Unauthorized disclosures of classified information by Members or staff should trigger thorough investigations relying on strict enforcement of the applicable Federal statutes and House rules. Any individual who is conclusively determined to be the source of such unauthorized disclosures should be subject to the full range of penalties prescribed by the law. The rules promulgated by the Committee on Standards of Official Conduct on July 12, 1995 should be strictly and consistently enforced by HPSCI.

- The current oversight structure puts intelligence -- as both a government function and as an issue -- at a distinct disadvantage. Unlike other national security functions, congressional oversight of intelligence is neither unified nor clearly delineated. The prime effect of this arrangement is seen in the degree to which intelligence programs are subjected to budget cuts largely because of *how* they are dealt with (i.e., as part of the defense authorization and appropriations process), rather than on their own merits.

Recommendations

- It is important that the House act to "normalize" the way in which it oversees intelligence. By continuing to handle intelligence as an extraordinary function, the current oversight system predicates an approach that may be overly adversarial and may actually make effective oversight more difficult.

- The House should give serious consideration to converting HPSCI to a standing committee, with no limits on terms of service for Members. This would help "normalize" intelligence and greatly improve expertise and continuity on the Committee.

- The House should consider allowing HPSCI to have exclusive jurisdiction over all aspects of intelligence that are part of the larger intelligence architecture, while the House National Security Committee (HNSC) has exclusive jurisdiction over those aspects of intelligence solely related to military intelligence needs but that are not part of this larger architecture. Second, the House should consider creating a separate appropriations subcommittee exclusively for intelligence.

- The House should seek to better protect Intelligence Community equities by erecting legislative "firewalls" between HPSCI and HNSC during the authorization phase; similarly, efforts should be made to establish mechanisms for better legislative consultation and coordination with the House Appropriations Committee during the appropriations phase.

- Establish a semi-annual strategic intelligence review meeting between the new Committee on Foreign Intelligence and the House and Senate intelligence committees.

CONGRESSIONAL OVERSIGHT

The modern system of congressional oversight of intelligence -- select committees in the House and in the Senate specifically devoted to intelligence -- is almost twenty years old. Reviewing the strengths and weaknesses of this system, as well as the contribution that congressional oversight can and should make to intelligence is appropriate as part of the larger *IC21* study.

Issues regarding congressional oversight fall into two large categories: the general nature of how Congress carries out oversight and specific issues of organization and process related to intelligence oversight. Although this report touches on some generic issues of intelligence oversight, its findings and recommendations are restricted to the way in which the House of Representatives handles this function.

Background: Evolution of Congressional Oversight of Intelligence

It is important to recall how the current intelligence oversight system came into being. The two select committees were the direct result of the congressional (and executive) investigations into U.S. intelligence activities in 1975-76. Both Houses came to the conclusion that the past oversight system had been inadequate in terms of both the vigor with which it was carried out[1] and the very limited number of Members who were privy to intelligence-related information. That older system reflected the gentleman's agreement nature of oversight that evolved during the Cold War. It accepted the necessity of intelligence -- and especially of intelligence activities (i.e., covert action), but treated them in an extraordinary manner because of their highly classified and extremely sensitive nature.

---

[1] The most-oft cited example of the problem was the quote from Senator Leverett Saltonstall, a member of the Armed Services Committee, which was responsible for intelligence oversight. When asked by Senator Mike Mansfield why there had only been two committee meetings with the CIA in the past year, Senator Saltonstall replied: "...it is not a question of reluctance on the part of the CIA officials to speak to us. Instead, it is a question of our reluctance, if you will, to seek information and knowledge on subjects which I personally, as a Member of Congress and as a citizen, would rather not have, unless I believed it to be my responsibility to have it because it might involve the lives of American citizens." *Congressional Record*, April 9, 1956, p. 5924.

The House Permanent Select Committee on Intelligence (HPSCI) was established on July 14, 1977 by H. Res. 658 of the 95th Congress and is governed by Rule XLVIII of the Rules of the House. The current system attempted to correct the main flaws in the older system in two major ways. First, the House decided that a committee with specific oversight over intelligence (albeit with different jurisdictions in the House and Senate) was necessary to ensure more vigorous and regular oversight. Second, in order to broaden the oversight base, each committee has "cross-over" Members from other committees that have an interest in intelligence or intelligence related issues: Appropriations; International Relations; Judiciary; and National Security.

However, and this is perhaps ironic, the House continued to treat intelligence as something extraordinary, rather than as an accepted function of government similar to any others that are subject to oversight. This is reflected in two aspects of HPSCI. First, it is a select committee rather than a standing committee. Second, and derived from the first, are the rules limiting the length of consecutive service on the Committee. These tenure rules arose from the perception that the past intelligence overseers had grown "too cozy" with the intelligence agencies, thus becoming less vigorous in their oversight. Rotating the membership on a regular basis, it was believed, would avoid this type of overly close and potentially less critical relationship in the future.

The Nature of Oversight: Adversary vs. Advocate

Each committee charged with congressional oversight has a dual responsibility. The most obvious is to oversee the various agencies under its mandate, approve their budgets, investigate known or suspected problems, and report back to the House on these matters. Recognizing the impossibility of each Member being conversant with (or intensely interested in) all issues, the committee system delegates responsibility to the committees and accepts their leadership in specific areas. Given the checks and balances nature of the congressional-executive relationship, each committee has, at some level, an adversarial role with its Executive Branch opposites. The relationship need not be overtly or continuously hostile, but there is inevitably a certain amount of friction involved.

The responsibility for being the House's resident experts on given programs and agencies also gives rise to a second role for each oversight committee, that of advocacy for those agencies and programs. It is only natural that those Members most interested in and most conversant with agencies and programs will also, on occasion, be their advocates. Increasingly constrained debates over budget shares, disinterest or outright hostility from other Members about agencies or programs for a wide variety of reasons, all put oversight committees in this advocacy role as well.

Oversight, if carried out properly, should be a combination of these two roles. An excessive concentration on either will damage the ability of the committee to handle its issues effectively and can undermine the credibility of that committee among its colleagues.

However, it is not clear that this norm of oversight behavior is widely accepted as proper for HPSCI. The fact that intelligence continues to be handled as an extraordinary issue in terms of oversight -- by virtue of a select committee and tenure limits -- suggests that it was at least expected at its origin that HPSCI would largely eschew advocacy role and that this expected emphasis on adversary rather than advocate has been tacitly accepted over the last twenty years.

There remains a lingering uneasiness about intelligence and its role in the U.S. government that will never be completely resolved. At some level, the concept of secret agencies with classified budgets runs counter to some deeply felt view of what and how the U.S. government should behave. However, this less than full acceptance may actually be heightened rather than pacified by the current oversight system, which treats intelligence in a manner different from other government activities.

Interestingly, several witnesses who appeared before HPSCI during *IC21* hearings made the same point: intelligence, unlike virtually all other functions of government, has no natural advocates in the public at large. Its direct effect on the lives of most citizens is largely unfelt or unseen; its industrial base is too rarefied to build a large constituency in many areas; it is largely an "inside the Beltway" phenomenon in terms of location, logistics, budget and concern. The only places where intelligence can hope to find some base level of support are from its Executive Branch masters and its congressional overseers.[2]

By having HPSCI as a select committee, Congress is, in effect, *elevating* intelligence. It is seen as an extraordinary issue requiring congressional organizational responses that depart from the norm. At some levels, this view of intelligence is accurate, but this also adds to the mystique that too often surrounds intelligence and often engenders wariness about it on the part of some Members. By making HPSCI a standing committee, intelligence would be treated like other "normal" functions of government. Making intelligence a less extraordinary issue might actually have positive effects, in that by being seen as less unique the very *raison* of the IC might not be questioned as much.

---

[2] Testimony of Richard Helms and James Schlesinger before House Permanent Select Committee on Intelligence on May 22, 1995.

The Propriety of Congressional Oversight of Intelligence

Not surprisingly, we believe that the modern oversight system for intelligence residing in committees specifically devoted to that task has worked well. The House and Senate committees have achieved the two main goals of their founders in the 94th and 95th Congresses, creating a system that is more vigorous and more rigorous and is more broadly based than the previous system. All oversight is imperfect and is always limited by the degree to which the Executive Branch will be forthcoming with information. Given the highly classified and often compartmented nature of intelligence information, this may be a more exacting problem for the intelligence committees. Nonetheless, we continue to believe that the current system has largely been effective.

We also do not see that any alternative to having a distinct committee oversee intelligence is preferable. Each oversight committee finds itself with a full agenda. Returning oversight to the House National Security Committee (HNSC) would act to the detriment of both those Members charged with intelligence oversight and the intelligence agencies themselves.

We also understand that there will always be some in the intelligence agencies who will question, resent and perhaps resist the idea of Congress having extensive oversight powers. This view is not unique to intelligence. It is unlikely that there is any Executive agency or department that does not harbor similar sentiments at some time. Still, this feeling may run deeper in the Intelligence Community. Sharing information with "outsiders," even if they are elected officials, runs counter to the ethos of intelligence as some understand it. We are also aware of repeated complaints by intelligence agency heads about the amount of time they must spend either before Congress or responding to Congress. Again, this sentiment is not unique, and we are also not convinced that the burden is any more onerous for intelligence agencies than for any others.

Effective oversight and an informed Congress are now considered among the expected norms of our system of government. We believe that oversight, if carried out seriously and with a modicum of support from intelligence agencies, not only helps ensure greater Executive branch effectiveness and propriety, but can also be a substantial force in rebuilding a sorely needed consensus to support intelligence agencies, programs and activities.

A Joint Committee

The issue of a joint congressional committee to oversee intelligence has been proposed in virtually every Congress since 1976. The main arguments in favor of a joint committee are:

- It would restrict the number of Members and staff (currently 33 Members and 50 staff in the House and Senate Committees) with access to highly classified information, thus limiting the possibility of unauthorized disclosures.

- It would underscore the seriousness with which Congress views intelligence, by handling it in this manner, similar to how atomic energy (i.e., nuclear weapons development and proliferation) issues were overseen from 1946-1977 by the Joint Committee on Atomic Energy.

The main arguments against a joint committee are:

- Concern over restricting the number of Members and staff with access to intelligence information implies that Congress cannot be trusted with such information. Although the record of Congress with regard to safeguarding such information is not perfect, it remains far better than Executive Branch agencies. Congress must be vigilant in this regard, but this does not argue that current number need to be further restricted.

- By creating a joint committee, Congress would further heighten the view that intelligence is an extraordinary, rather than an accepted, function of government. No other executive branch agencies or functions are overseen by a joint committee, thus raising the issue of why intelligence needs to be overseen in this manner.

- The oversight scope of the two current intelligence committees are not identical. Intelligence programs are currently divided into three broad groups: *NFIP: the National Foreign Intelligence Program*, which includes the Director of Central Intelligence; CIA; and the national foreign intelligence or counterintelligence programs of the Defense Department, DIA, NSA, the Central Imagery Office, NRO, Army, Navy and the Air Force, the Departments of State, Treasury and Energy, the FBI and DEA; *JMIP: the Joint Military Intelligence Program*, covering intelligence for defense-wide or theater-level consumers; and *TIARA: Tactical Intelligence and Related Activities,* covering service unique and tactical intelligence needs. HPSCI oversees all of these intelligence programs, sharing oversight of TIARA with the HNSC. The Senate Select Committee on Intelligence (SSCI) oversees only the NFIP. To create a joint committee, one House or the other would have to make substantial changes in the scope of oversight accorded to this new committee.

- It is highly questionable that the establishment of a joint committee would significantly reduce the number of Members and staffers that currently have access to classified information. No committee system will make Congress "leak proof." Even with a joint committee, there still would be a substantial number of Members and staff with access to intelligence information across several House Committees (Appropriations, National Security, Judiciary, International Relations), as well as their Senate counterparts.

- The joint committee structure is not suitable to an authorizing committee as it would complicate Congressional efforts to conduct our necessary oversight activities. By shrinking the number of Members familiar with the Intelligence Community, an inevitable result will be a diminution in Members' knowledge of the complexities of intelligence oversight. Additionally, the current system of two separate intelligence committees provides a more effective system of Constitutional checks and balances on Executive Branch activities.

Finding: There is no compelling reason to convert the current system to a joint committee. As noted, Congress's record regarding safeguarding highly classified information is not perfect, but does not warrant this step. Creating a joint committee would also require either the House or the Senate to alter its current arrangements for intelligence oversight, which has not had significant support in the past. Finally, and most importantly, creating a joint committee for intelligence would continue to heighten the view that intelligence is something other than an accepted function of government, which tends to increase rather than complement oversight issues and problems.

Select Committee/Appointment and Tenure Limits

The reasons for these two aspects of the current oversight structure are described above. Although specific provisions for a standing intelligence committee could be established, changing HPSCI into a standing committee would *most likely* (but not necessarily) affect the process of assignment and lengths of service.

The main arguments in favor of the current select committee arrangement relating to assignment procedures are:

- Intelligence activities are inherently different from other areas of government; secrecy is a paramount consideration on which depends the lives of agents attempting to assist the United States. Further, intelligence gathering deals with highly sensitive sources and methods of collection and analysis. The Speaker and Minority Leader already have special statutory standing to be advised of covert actions; allowing them to select Members of HPSCI is consistent with this prerogative and serves to increase the likelihood that only those with a demonstrated commitment to preserving the secrecy of classified information will be placed in oversight of intelligence agencies.

- Given the sensitivity of the Committee's work, Members who are unwilling to maintain the secrecy of classified information, despite the secrecy oaths required by House rules, should be removable without the necessity of contentious caucus votes. Maintaining the select committee status allows the Speaker to act with dispatch to remove Members who do not maintain the secrecy of classified materials. This approach underscores the view that intelligence must be handled in an extraordinary manner.

The main arguments in favor of the current select committee arrangement relating to the length of member service are:

- Limiting service on HPSCI, in accordance with the current rule, to four terms (five for the chairman and ranking member) reduces the likelihood that Members will become "clients" of intelligence agencies, less rigorous in their oversight, or that they will be able unfairly to direct intelligence spending to their home districts. It also increases the likelihood that Members will reflect the diversity of public opinion regarding intelligence issues.

- Inasmuch as information available to HPSCI cannot be made available to all Members, rotating service will permit a larger percentage of Members to have some understanding of intelligence issues. For example, there are currently some 20 Members of the House who have previously served on the HPSCI, including three former chairmen. Such experience contributes to better informed decisions on intelligence budgets as well as on national security questions that require an appreciation for the limits of available intelligence information.

- Limiting length of service is consistent in spirit with widespread popular support for "citizen legislators" and with actions taken in the 104th Congress to limit the tenures of committee and subcommittee chairmen as opposed to the previous reliance on seniority.

There are three primary attributes that most observers would acknowledge as differentiating select and standing committees: (1) Speaker appointments vs. caucus/conference appointments; (2) limited vs. permanent tenure; and (3) study and review authority vs. permanent jurisdiction. The main arguments supporting the establishment of a standing committee relating to assignment procedures are as follows:

- Intelligence is a normal function of government and is integral to the conduct of foreign policy and military operations. Creation of a standing intelligence committee would recognize this reality and demonstrate to the public the determination of Congress to provide appropriate oversight of sizable Federal agencies.

- HPSCI deals with policy questions not essentially different from other committees and should, like them, reflect the spectrum of views held by Members.

- Noting the unique scope and responsibilities involved in intelligence oversight, the Speaker should retain a central role in appointing Members to the new standing intelligence committee, as is the case under the select committee arrangement (see Rule X, clause 6, paragraph (f)). The Speaker should also retain the power he currently has to remove Members. Members of the standing intelligence committee should not, however, be removable by a Speaker who may be pursuing a political agenda. While these conditions would be unique among the House's standing committees, it may be appropriate for the committee's leadership to seek a waiver of the requirement that membership be appointed by the House from nominations made by party caucuses.

- As is the case with the Budget Committee, there could be a continuing requirement that some Members on the standing intelligence committee also serve on other specified committees with jurisdictions related to intelligence (*e.g.,* National Security, International Relations, or Judiciary). A new standing intelligence committee would have to grapple with the issue of "crossover" Members from the National Security, International Relations, Judiciary and Appropriations Committees. These Committees were guaranteed seats on HPSCI as part of their loss of some oversight responsibilities.

- In standing committees, other than the Budget Committee, there are no limitations on length of service and seniority is usually the basis for appointment as chairman and ranking minority member. Effective with the 104th Congress, committee and subcommittee chairmen are limited to no more than three consecutive terms of service as committee leaders. Again noting the unique scope and responsibilities involved in intelligence oversight, it may be prudent for the Committee's leadership to seek a waiver of this tenure requirement.

- If HPSCI became a regular standing committee, then membership on it would be counted against the number of committee and subcommittees on which a Member could serve. This could be a difficult decision given the minimal amount of constituent interest likely to be found in intelligence matters. Such a change would also mean that members of "exclusive" committees, such as Appropriations, could no longer serve on the standing intelligence committee -- which could be a major loss in terms of easing the authorization/appropriations process. In addition, the overlap of Members from the "exclusive" committees ensures that intelligence concerns and needs receive sufficient attention from the National Security, International Relations, Judiciary, and Appropriations Committees.

- Finally, there is the issue of HPSCI Members not getting too comfortable or familiar with the Intelligence Community. This view is a direct outgrowth of the congressional investigations of the mid-1970s, which concluded that the former intelligence overseers (in the Senate Armed Services Committee and House Armed Services Committee) had become lax, in part by virtue of being too "cozy" with the Intelligence Community. Interestingly, this is not seen as a being a problem vis-a-vis HNSC or the Senate Armed Services Committee (SASC) and the military, nor between Judiciary and the FBI.

The main arguments in favor of a standing committee arrangement relating to the length of member service are:

- Tenure limits under the current select committee process make it less likely that Members will become overly familiar with intelligence agencies, thus possibly diminishing the rigor of oversight.

- The current tenure limits have also been responsible to some degree for the rapid change in HPSCI chairmen since the initial tenure of Chairman Boland. Since he stepped down in 1985, there have been six chairmen. This has obvious costs in terms of continuity and, in effect, makes the staff much more responsible for that important and unseen facet of committee life. Some observers have argued that the rapid rotation of HPSCI chairmen makes consistent oversight more difficult.

- Limiting service on the Committee to four terms (or five for the chairman and ranking member) does not allow HPSCI to benefit adequately from Members' experience in the arcane world of intelligence, especially the complicated relationships among the agencies, the role of the DCI, and complex and separate budgeting procedures for national and tactical programs. Members acquire experience in intelligence behind closed doors at the expense of other duties and this experience should be fully utilized in overseeing intelligence activities. A significant portion of a six or eight year term on the Committee must be spent mastering intelligence, with less time left to use that expertise. This, in turn, makes Members of HPSCI much more dependent on the staff, who provide the greatest available base of institutional knowledge and continuity.

- Removal of the tenure limits would also allow the Committee to have a membership that is more consistently conversant with intelligence issues. This has not been an issue in the 104th Congress. However, in the 103rd Congress, 11 of 19 Members were new to HPSCI. As previously noted, this might also lead to greater stability in the chairmanship, assuming some continuity by one party.

- Even though HPSCI is a relatively new committee, existing term limits have already been overridden on several occasions to permit appointment of experienced Members to additional service on the Committee. The practice of Members leaving the Committee and subsequently returning in order to stay within restrictions has been criticized by some as contrary to the spirit of the House rules, although it has the benefit of providing Members who are enthusiastic and knowledgeable.

- More important changes would likely come in the Committee's membership. Assuming that the tenure limitations were abandoned, service on a standing intelligence committee might become more attractive. Currently, service on HPSCI has more overt drawbacks than attractions: it likely offers no help vis-a-vis the interests of the Members' districts; it detracts time and attention from issues of direct interest to constituents; and there is little Members can say about what they do on HPSCI. None of these would be likely to change. However, if service on the Committee offered a more reasonable prospect of a subcommittee chairmanship or Committee chairmanship over time, then this would be a new and major attraction.

Finding: Although the reasons for which HPSCI was made a select committee with tenure limits may have been valid in 1977, these may no longer be compelling or valid. There are equally compelling arguments in terms of the general effect of these arrangements on oversight to warrant reconsidering them and to proceed with the establishment of a standing intelligence committee. In doing so, significant efforts should be made to secure the presence of "crossover" Members from the National Security, International Relations, Judiciary and Appropriations Committees within the standing committee's membership.

Unauthorized Disclosure: Members and Staff

The ability to safeguard highly classified information with which it has been entrusted is an issue for several committees, not just HPSCI. As noted, no committee can boast a perfect record in this regard, although the record of any congressional committee is far superior to the Executive Branch national security agencies. This does not excuse leaks from Congress, but it should serve to put in perspective the false complaints too often heard from Executive Branch officials about their inability to trust Congress.

There are two views on the responsibility imposed on Congress by the receipt of classified information. There is general agreement that access to such information is necessary for Congress to carry out effective oversight. Some argue that Congress is responsible for engendering some degree of trust in how it handles this information so that Executive agencies will be forthcoming. Others reject this view, arguing that it is up to Executive agencies to win the trust of Congress and that these agencies have no choice but to provide Congress with the information it requires.

With the advent of the 104th Congress, Members of HPSCI now take two oaths regarding the safeguarding of information, one as Members of the House and one as Members of the Committee. Some argued that there was some ambiguity in these

oaths; we believe that the letter and the ruling issued by the Committee on Standards of Official Conduct on July 12, 1995 offered important clarifications. That Committee noted first that HPSCI's Classified Information Oath embraces "any classified information provided to a Member by any person during the Member's term in office." Second, the Committee on Standards of Official Conduct imposed upon Members an affirmative duty to inquire whether sensitive information in that Member's possession is indeed classified before disclosing it to the public.

HPSCI staff undergo background investigations and are subject to the Rules of the House (see Rule XLIII, clause 13) regarding unauthorized disclosure of information. Some, primarily from the Executive Branch, have argued that at least staff, and perhaps Members, should be subject to the same security requirements as Executive Branch officials, particularly, a requirement to submit to comprehensive polygraph examinations on a regular basis. These remain controversial tools within the Executive Branch; there is no one standard for polygraphs nor is there a uniform policy among all Executive Branch agencies.

> **Finding:** Unauthorized disclosures of classified information by HPSCI Members or staff should result in swift and sure penalties against any individual who is conclusively determined to be the source of such disclosures. The rules promulgated by the Committee on Standards of Official Conduct on July 12, 1995 should be strictly enforced by HPSCI.

Jurisdiction

Select committees usually do not have exclusive jurisdiction over an area of government. Standing committees usually do have exclusive jurisdiction although there are considerable areas of overlap among standing committees. Select committees usually do not have the legislative authority to report legislation to the floor. HPSCI already has authority to report legislation and this would presumably not be altered if it became a standing committee.

One of the more difficult aspects of intelligence oversight is the fact that budget authorization for and some degree of general oversight of intelligence is divided between committees. This shared jurisdiction between HPSCI and HNSC derives from two factors.

First, HNSC (then called Armed Services) had been the committee charged with intelligence oversight prior to 1977. The decision to continue some shared jurisdiction, at least over the TIARA portion of intelligence, allowed HNSC to preserve some of its jurisdiction. Second, the decision reflected the view that, given the importance of intelligence to military operations and the fact that the classified portion of the intelligence budget is lodged within the larger defense budget, this sharing was also appropriate.

Nothing has happened to undercut these rationales, but it is important also to look at the effects of this shared oversight on intelligence. There are two major problems -- the effect on the creation of the overall intelligence budget and the extraneous pressures that are brought to bear on the intelligence budget.

HPSCI is charged with authorizing a global intelligence architecture, i.e., the entire range of intelligence programs from TIARA up through the national programs. This architecture is supposed to be coherent and mutually supportive. This becomes difficult, from the standpoint of HPSCI, when a significant portion of this budget is, in effect, authorized twice and not always at the same levels. Replicating the Senate intelligence oversight system, wherein SSCI has no oversight functions regarding TIARA, would be one solution, but it would undercut the goal of creating a global intelligence architecture. The other solution would be to cede exclusive oversight to HPSCI of those systems designed to gather intelligence as part of this larger architecture, reserving to HNSC those parts of TIARA that are exclusively related to military intelligence needs but are not part of this larger architecture.

The second issue derives from the fact that the intelligence budget remains classified and is "hidden" within the larger defense budget for both authorization and appropriation. HNSC divides the budget into functional categories: procurement, research and development, etc. None of these is a "logical" place to house the intelligence budget. In actuality, the defense and intelligence authorization processes move along parallel but unrelated tracks. When the intelligence budget is completed, it is then hidden within HNSC Subcommittee budgets. As these National Security functions then move through the congressional budget process they inevitably come under pressure for a variety of reasons. If, for example, the dominant view becomes that the research and development budget is too high -- and intelligence is hidden within that budget function -- then intelligence must take its "fair share" of reductions for reasons entirely extraneous to the merits of the intelligence programs. Moreover, as the entire intelligence budget is hidden in this manner, all programs are liable to such cuts, not just TIARA.

Making HPSCI a standing committee would not in and of itself extend its exclusive jurisdiction over intelligence matters, and specifically, the Central Intelligence Agency and the Director of Central Intelligence. However, HNSC would retain oversight over the Department of Defense (DoD), which conducts both national and tactical intelligence operations. The State Department, including the Bureau of Intelligence and Research, would continue to be overseen by the House International Relations Committee, and there would be additional overlap in other areas. HPSCI also has concurrent jurisdiction in specified areas with the Judiciary Committee and the Committee on Space and Science, and Technology.

With the reduced structure and personnel levels in DoD, emphasis on equipping the military with the highest-technology weapons and support systems, the emphasis

on "support to the warfighter" and "support to military operations," that has permeated the defense and intelligence thought process, and the overall drive to achieve a balanced budget, the accepted practice of competing weapons and intelligence programs will not only likely continue, but could well grow. Those who argue that this process is justified, often point out that the majority of expenditures within the intelligence budget are within defense and that the reliance of newer systems on intelligence will properly balance out the trade-offs.

Were we structuring intelligence to operate effectively to support only tactical operations, these arguments might be more compelling. But, it is increasingly clear that emphasis on strategic or baseline intelligence -- intelligence regarding a broader picture, not intelligence on strategic weapons systems -- is becoming more important to the policy maker and to the military commander, as it will allow us to avoid confrontations, plan operations, and respond to the unexpected issues that are increasingly part of our foreign policy, in a manner that is less reactive. If successful, such intelligence planning and operations can reduce the risk to U.S. military forces.

Without adequate safeguards in the appropriations process, however, intelligence programs will continue to be subjected to those who have strong constituency interests in national security and the defense industry. The FY96 intelligence budget is a relevant case in point. For the first time in several years, HPSCI passed an intelligence budget that represented an increase in spending. The budget had bipartisan support and reflected the Committee's approach of beginning the process of planning for the future. Yet, during the appropriations process, when it was determined that there were significant overages in specific intelligence accounts, money was first taken out of intelligence to pay for specific weapons systems rather than being considered available to better fund other intelligence programs or operations. Likewise, intelligence funding is being sacrificed by the Clinton Administration in order to pay for non-intelligence military operations in Bosnia. The continued process of raiding the intelligence budget in order to pay bills within the military tends to be short-sighted and will serve only to inhibit effective intelligence operations in the future -- a fact that will ultimately increase the risk to U.S. forces and national security.

Although many of the budget battles on intelligence programs are fought within the authorization process and, as identified elsewhere in *IC21* staff studies, steps must be taken to "clean up" the various budget accounts (especially, JMIP and TIARA) to help coordination between the authorization committees, the wars are actually won or lost in the appropriations process. Therefore, designing safeguards within the House Appropriations Committee could be central to successful intelligence operations and support in the 21st century.

Currently, the intelligence budget is reviewed and acted upon by the National Security Subcommittee of the House Appropriations Committee, along with most of

the rest of the defense budget. Such a structure allows -- in fact, encourages -- trade-offs to be made within the entirety of the defense budget, including intelligence. One option to help protect necessary intelligence equities might be a separate subcommittee on intelligence. Such a subcommittee would be responsible for review of the NFIP and JMIP budgets, leaving the TIARA budget review within the National Security Subcommittee. This would help protect "national" and "defense-wide" intelligence assets, while leaving those intelligence assets that are integral to service operations to be considered with the forces for which they are a part. (This assumes that there is a restructuring of the JMIP and TIARA programs as discussed elsewhere in *IC21* studies.) The result would be a better protected, more coherent look at the intelligence budget, with trade-offs being made against intelligence resources rather than with non-intelligence, defense programs. The ability to focus trade-offs -- and, thus, planning -- within intelligence, also provides the ability to better understand the effects of such trade-offs more in terms of the synergy of our overall intelligence capabilities.

> **Finding:** The current oversight structure puts intelligence -- as both a government function and as an issue -- at a distinct disadvantage. Unlike other national security functions, congressional oversight of intelligence is neither unified nor discreet. The prime effect of this arrangement is seen in the degree to which intelligence programs are subjected to budget cuts largely because of *how* they are dealt with (i.e., as part of the defense authorization and appropriations process), rather than on their own merits. Therefore, serious consideration ought to be given to establishing a separate subcommittee on intelligence within the House Appropriations Committee and to shift a number of the current functions of the existing Appropriations Subcommittee on HNSC to this new subcommittee.

Linkages Between HPSCI and the New Committee on Foreign Intelligence

In separate *IC21* studies, it has been proposed to create a new, high-level Committee on Foreign Intelligence (CFI) to enhance oversight of the Intelligence Community as well as to better focus the Community's collection and analytical capabilities. The new CFI is to be composed of senior Executive Branch policy makers who would advise the DCI on national intelligence priorities. Noting the sensitivity and importance of the CFI's role, it may be prudent to consider whether a regular oversight dialogue should be established between the CFI and the intelligence committees. A semi-annual strategic intelligence review meeting between the CFI and the intelligence committees might improve the flow of information and dialogue between the Executive and Legislative Branches on significant intelligence matters.

> **Finding:** Establish a semi-annual strategic intelligence review meeting between the new Committee on Foreign Intelligence and the intelligence committees.

Conclusion: Findings and Recommendations

Findings

- The current intelligence oversight system arose from a view that intelligence had to be handled in a manner that was extraordinary when compared to other functions of government. Although that view may have been warranted in the aftermath of the investigations in 1975-76, it is not warranted any longer. Indeed, by continuing to view intelligence in this manner, oversight and the work of the Intelligence Community are likely made more difficult.

- Advocacy for overseen agencies is legitimate and to some extent necessary. This has not been an accepted stance for the intelligence committees. We agree with the view of former DCIs that intelligence is such a restricted issue that Congress must be more active in building the necessary political consensus.

- The current oversight system has been largely effective, and clearly has responded to those problems that prompted the creation of the current committees.

- There is no compelling reason to convert the current system to a joint committee. As noted, Congress's record regarding safeguarding highly classified information is not perfect, but does not warrant this step. Creating a joint committee would also require either the House or the Senate to alter its current arrangements for intelligence oversight, which has not had significant support in the past. Finally, and most importantly, creating a joint committee for intelligence would continue to heighten the view that intelligence is something other than an accepted function of government, which tends to increase rather than complement oversight issues and problems.

- Although the reasons for which the current committee was made a select committee with tenure limits may have been valid in 1977, these may no longer be compelling or valid. There are equally compelling arguments in terms of the general effect of these arrangements on oversight to warrant reconsidering them.

- Unauthorized disclosures of classified information by Members or staff should trigger thorough investigations relying on strict enforcement of the applicable Federal statutes and House rules. Any individual who is conclusively determined to be the source of such unauthorized disclosures should be subject to the full range of penalties prescribed by the law. The rules promulgated by the Committee on Standards of Official Conduct on July 12, 1995 should be strictly and consistently enforced by HPSCI.

- The current oversight structure puts intelligence -- as both a government function and as an issue -- at a distinct disadvantage. Unlike other national security functions, congressional oversight of intelligence is neither unified nor clearly delineated. The prime effect of this arrangement is seen in the degree to which intelligence programs are subjected to budget cuts largely because of *how* they are dealt with (i.e., as part of the defense authorization and appropriations process), rather than on their own merits.

Recommendations

- It is important that the House act to "normalize" the way in which it oversees intelligence. By continuing to handle intelligence as an extraordinary function, the current oversight system predicates an approach that may be overly adversarial and may actually make effective oversight more difficult.

- The House should give serious consideration to converting HPSCI to a standing committee, with no limits on terms of service for Members. This would help "normalize" intelligence and greatly improve expertise and continuity on the Committee.

- The House should consider allowing HPSCI to have exclusive jurisdiction over all aspects of intelligence that are part of the larger intelligence architecture, while the HNSC has exclusive jurisdiction over those aspects of intelligence solely related to military intelligence needs but that are not part of this larger architecture. Second, the House should consider creating a separate appropriations subcommittee exclusively for intelligence.

- The House should seek to better protect Intelligence Community equities by erecting legislative "firewalls" between HPSCI and HNSC during the authorization phase; similarly, efforts should be made to establish mechanisms for better legislative consultation and coordination with the House Appropriations Committee during the appropriations phase.

- Establish a semi-annual strategic intelligence review meeting between the new Committee on Foreign Intelligence (CFI) and the intelligence committees.

APPENDIX A

IC21 Hearings and Witnesses

May 22, 1995: *IC21*: Directors of Central Intelligence

Witnesses
The Honorable Richard Helms
The Honorable James Schlesinger
The Honorable William E. Colby
The Honorable Stansfield Turner
The Honorable William H. Webster
The Honorable R. James Woolsey

July 13, 1995: Future of Technology

Witnesses
Mr. Bill Richardson, Director Advanced Technologies Office, DCI's Community Management Staff
Dr. Lee Buchanan, Director Defense Sciences Office, Advanced Research Projects Agency
Dr. Curtis R. Carlson, Executive Vice President, David Sarnoff Research Center

July 27, 1995: Policy Makers and Intelligence

Witnesses
Lieutenant General Brent Scowcroft, Former National Security Advisor
Ambassador Robert Kimmitt, Former Ambassador to Germany and Under Secretary of State for Political Affairs
Dr. Joseph Massey, Former Assistant U.S. Trade Representative

October 18, 1995: Enabling Technologies

Witnesses
The Honorable Paul G. Kaminski, Under Secretary of Defense for Acquisition and Technology
Mr. Norman Augustine, President of Lockeed-Martin Corportation
Mr. Edward McCracken, Chairman and CEO of Silicon Graphics Incorporated

November 16, 1995: Intelligence Community "Wise Men"

Witnesses
Mr. John N. McMahon, Former Deputy Director of Central Intelligence
Mr. Richard J. Kerr, Former Deputy Director of Central Intelligence
Lieutenant General James R. Clapper (Retired) Former Director of the Defense Intelligence Agency

December 19, 1995: *IC21*: Director of Central Intelligence

Witness
The Honorable John M. Deutch, Director of Central Intelligence

APPENDIX B

IC21 Staff Panels

In addition to six full Committee *IC21* hearings, the staff conducted dozens of interviews with Intelligence Community experts and held several staff panels. Following are a list of the staff panels:

SIGINT: Signals Intelligence

PANEL ON CRYPTOLOGY IN THE 21ST CENTURY: Participants included representatives from the National Security Agency (NSA).

PANEL ON THE FUTURE OF THE SERVICE CRYPTOLOGIC ELEMENTS: Participants included representatives from the Army Security Agency, Air Intelligence Agency, Naval Security Group, and Marine Support Battalion.

IMINT: Imagery Intelligence

PANEL 1: Participants included representatives from the National Photographic Interpretation Center (NPIC), Defense Intelligence Agency (DIA), and Defense Mapping Agency (DMA).

PANEL 2: Participants included representatives from the U.S. Air Force, U.S. Army, U.S. Navy, U.S. Marine Corps, the military service J-2s, the office of the Secretary of Defense (OSD), and the office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD/C3I).

PANEL 3: Participants included representatives from the National Information Display Laboratory, National Exploitation Laboratory, and Advanced Research Programs Agency.

MASINT: Measurement and Signatures Intelligence

PANEL 1: Participants included representatives from the Central MASINT Office (CMO), Office of the Secretary of Defense (OSD), U.S. Marine Corps, Arms Control and Disarmament Agency (ACDA), Department of the Army/Military Intelligence (DAMI), and Office of Naval Intelligence (ONI).

PANEL 2: Participants included representatives from the Non-Proliferation Center (NPC), Office of Technical Collection (CIA/OTC), Community Requirements and Evaluation Staff (CIA/CRES), National Security Agency (NSA), and U.S. Air Force (USAF).

PANEL 3: Participants included representatives from the Office of Naval Intelligence (ONI), Department of the Army/Military Intelligence (DAMI), Arms Control and Disarmament Agency (ACDA), Community Requirements and Evaluation Staff (CIA/CRES), Central MASINT Office (DIA/CMO), National Security Agency (NSA), U.S. Marine Corps, U.S. Air Force, and the office of the Secretary of Defense for Command, Control, Communications and Intelligence (OSD/C3I).

Clandestine Service

PANELS: Three panels were held with present and former CIA/Directorate of Operations (DO) case officers and other intelligence officials.

Intelligence Community "Surge" Capability

PANEL: Participants included representatives from the National Military Intelligence Production Center (NMIPC) and the Directorate of Intelligence (CIA/DI).

Congressional Research Service • The Library of Congress • Washington, D.C. 20540-7000

Proposals for Intelligence Reorganization, 1949-1996

(A Report Prepared for the Permanent Select Committee on Intelligence, House of Representatives)

Richard A. Best, Jr.
Analyst in National Defense
and
Herbert Andrew Boerstling
Research Assistant
Foreign Affairs and National Defense Division

February 28, 1996

TABLE OF CONTENTS

INTRODUCTION 1

PART I 4
Intelligence Reform Proposals Made by Commissions and Major Legislative Initiatives 4
- The Truman Administration, 1945-1953 4
- The First Hoover Commission, 1949 5
- Intelligence Survey Group (Dulles-Jackson-Correa Report), 1949 7
- Summary of the Truman Administration Intelligence Investigations 9
- The Eisenhower Administration, 1953-1961 9
- Second Hoover Commission, 1955 9
- The Doolittle Report, 1954 11
- Bruce-Lovett Report, 1956 12
- Summary of the Eisenhower Administration Intelligence Investigations 13
- The Kennedy Administration, 1961-1963 14
- The Taylor Commission 14
- The Kirkpatrick Report 16
- Summary of the Kennedy Administration Intelligence Investigations 17
- The Johnson Administration, 1963-1969 17
- The Nixon Administration, 1969-1974 17
- The Schlesinger Report, 1971 17
- Summary of the Nixon Administration Intelligence Investigation 18
- The Era of Public Investigations, 1974-1981 19
- Murphy Commission, (Commission on the Organization of the Government for the Conduct of Foreign Policy), 1975 19
- Rockefeller Commission (Commission on CIA Activities within the United States), 1975 21
- Church Committee (Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities), 1976 23
- Pike Committee (House Select Committee on Intelligence), 1976 26
- Clifford and Cline Proposals, 1976 27
- Proposed Charter Legislation, 1978-1980 28
- The Executive Branch Response, 1976-1981 29
- The Turner Proposal, 1985 31
- Iran-Contra Investigation, 1987 31
- Boren-McCurdy, 1992 32
- Commission on the Roles and Capabilities of the U.S. Intelligence Community (Aspin Commission), 1995-1996 33

PART II 35
Advantages and Disadvantages of Major Proposals 35
- Role of the DCI 37
- Role of the CIA Operations Directorate 39
- Disclosing the Intelligence Budget 41

Conclusion 43

PROPOSALS FOR INTELLIGENCE REORGANIZATION, 1949-1996

SUMMARY

Proposals for the reorganization of the United States Intelligence Community have repeatedly emerged from commissions and committees created by either the executive or legislative branches. The heretofore limited authority of Directors of Central Intelligence and the great influence of the Departments of State and Defense have inhibited the emergence of major reorganization plans from within the Intelligence Community itself. The history of efforts--successful and otherwise --to reorganize the U.S. Intelligence Community can be largely traced in the proposals of outside commissions set up to investigate perceived shortcoming in intelligence capabilities.

Proposals to reorganize the Intelligence Community date to the period immediately following passage of the National Security Act of 1947 (P.L. 80-253) that established the position of Director of Central Intelligence (DCI) and the Central Intelligence Agency (CIA). Recommendations have ranged from adjustments in the DCI's budgetary responsibilities to the actual dissolution of the CIA and returning its functions to other departments. The goals underlying such proposals have reflected trends in American foreign policy and the international environment as well as domestic concerns about governmental accountability.

In the face of a hostile Soviet Union, early intelligence reorganization proposals were more concerned with questions of efficiency. In the Cold War context of the 1950s, a number of recommendations sought aggressively to enhance U.S. covert action and counterintelligence capabilities. The chairman of one committee charged with investigating the nation's intelligence capabilities, Army General James H. Doolittle, argued that sacrificing America's sense of "fair play" was wholly justified in the struggle to prevent Soviet world domination.

Following the failed invasion of Cuba at the Bay of Pigs, the unsuccessful results of intervention in Vietnam, and the Watergate scandal, investigations by congressional committees focused on the propriety of a wide range of heretofore accepted intelligence activities that included assassinations and some domestic surveillance of U.S. citizens. Some forcefully questioned the viability of secret intelligence agencies within a democratic society. These investigations resulted in much closer congressional oversight and a more exacting legal framework for intelligence activities. At the same time, the growth in technical intelligence capabilities led to an enhanced--but by no means predominant--leadership role for the DCI in determining community-wide budgets and priorities.

With the end of the Cold War, emerging security concerns, including transnational terrorism, narcotics trafficking, and proliferation of weapons of mass destruction, face the United States. Most recent proposals for intelligence reorganization address post-Cold War requirements for covert action, the structure and size of the CIA, and the extent of the DCI's authority over all elements of the Intelligence Community. These post-Cold War issues can be usefully addressed with an awareness of arguments *pro* and *con* that were raised by earlier investigators.

PROPOSALS FOR INTELLIGENCE REORGANIZATION, 1949-1996

INTRODUCTION

The National Security Act of 1947 (P.L. 80-253) established the statutory framework for the managerial structure of the United States Intelligence Community, including the Central Intelligence Agency (CIA) and the position of Director of Central Intelligence (DCI). A fundamental intent of this legislation was to coordinate, and to a certain extent centralize, the nascent intelligence efforts of the United States as an emergent superpower in the face of a hostile Soviet Union. In addition, the act provided the CIA with the ability to assume an operational role by charging it with:

> Perform[ing] such other functions and duties related to intelligence affecting the national security as the National Security Council may from time to time direct.[1]

In 1947, the foundation of the present-day Intelligence Community consisted only of the relatively small intelligence components in the Armed Services, the Departments of State and the Treasury, the Federal Bureau of Investigation (FBI), and the fledgling CIA. Since 1947, however, the Intelligence Community "has greatly expanded in size and acquired a much broader range of responsibilities in the collection, analysis, and dissemination of foreign intelligence."[2]

The U.S. Intelligence Community is defined by the Fiscal Year 1996 Intelligence Authorization Act (P.L. 104-93). It listed the following agencies and organizations that conduct intelligence and intelligence-related activities:

Central Intelligence Agency
Department of Defense
Defense Intelligence Agency
National Security Agency
National Reconnaissance Office
Departments of the Army, Navy, Air Force
Department of State
Department of the Treasury
Department of Energy
Federal Bureau of Investigation
Drug Enforcement Administration
Central Imagery Office.

---

[1]Section 102(d)(5), National Security Act of 1947, P.L. 80-253; hereafter cited as National Security Act of 1947.

[2]Congressional Research Service. Alfred B. Prados, *Intelligence Community Leadership: Development and Debate Since 1947*, CRS Report 89-414 F, June 27, 1989, p. 1; hereafter cited as Prados, 89-414 F.

Beginning in January 1948, numerous independent commissions, individual experts, and legislative initiatives have examined the growth and evolving mission of the Intelligence Community. Proposals by these groups have sought to address perceived shortcomings in the Intelligence Community's structure, management, role, and mission. These proposals have ranged in scope from basic organizational restructuring to, more recently, the dissolution of the CIA.

In 1948 and 1949, two executive branch commissions examined the intelligence and operational missions of the CIA, and identified fundamental administrative and organizational loopholes in P.L. 80-253. By the 1950s, however, the physical growth and evolving mission of the Intelligence Community led subsequent commissions to broaden the scope of their proposals to include the enhancement of the DCI's community-wide authority, and the establishment of executive and legislative branch intelligence oversight committees. Unlike the intelligence investigations of the 1970s and 1980s, these early studies were primarily concerned with questions of efficiency and effectiveness rather than with issues of legality and propriety.

Following the Vietnam War and "Watergate," investigatory bodies became increasingly critical of the national intelligence effort. Beginning in the mid-1970s, the impetus shifted to the legislative branch where investigatory committees led by Senator Frank Church and Representative Otis G. Pike issued a broad range of proposals, including the separation of the DCI and CIA Director positions, dividing the CIA's analytical and operational responsibilities into two separate agencies, and the establishment of congressional oversight committees. In 1976 and 1977, respectively, recommendations by the these committees led to the establishment of the Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI). These committees were heavily involved in the investigations into the Iran-Contra affair of the mid-1980s.

With the end of the Cold War, and in the wake of the Aldrich Ames espionage case, both the executive and legislative branches are currently undertaking studies to determine the future roles, capabilities, management, and structure of the Intelligence Community. These studies include such issues as the need to maintain the CIA as a separate entity, the extent and competence of U.S. counterintelligence (CI) efforts, and the managerial structure of intelligence components in the armed services and the Department of Defense (DOD). A comprehensive examination of the DCI's roles, responsibilities, authorities, and status is also being undertaken. In an era of budgetary constraints and shifting policy concerns, these studies are also examining personnel issues, allocation of resources, duplication of services, expanded use of open source Intelligence (OSCINT), and the need for maintaining a covert action (CA) capability.

In the course of recurring proposals for altering the organization of the Intelligence Community, the forty-eight year history of these investigations has witnessed the gradual transformation of intelligence from a White House asset to one that is shared between the executive and legislative branches. Congress not only has access to intelligence judgments but to most information that intelligence agencies acquire as well as the details of intelligence activities. Congress has accepted some responsibility as a participant in the planning and conduct of covert actions. In significant measure, this process has been encouraged by these external intelligence investigations.

This report provides a chronological overview and examination of the major executive and legislative branch intelligence investigations made from January 1949 to date. In Part

I, all major proposals are listed in chronological order with a brief discussion of their respective results. In Part II, these proposals are grouped together by issues and include an examination of arguments for and against. Proposals specifically relating to congressional oversight of the Intelligence Community are not included in this report.

PART I

Intelligence Reform Proposals Made by Commissions and Major Legislative Initiatives

Alice soon came to the conclusion that it was a very difficult game indeed.
-Lewis Carroll, *Alice's Adventures In Wonderland*[3]

The Truman Administration, 1945-1953

Following the Second World War, the United States emerged as a global political, military, and economic leader. In the face of Soviet aggressiveness, the U.S. sought to enhance its national defense capabilities to curb the international spread of communism and to provide security for the nation itself.

The National Security Act (P.L. 80-253), signed July 26, 1947, established the statutory framework for the managerial structure of the United States Intelligence Community, including the Central Intelligence Agency (CIA) and the position of Director of Central Intelligence (DCI). The Act also created a semi-unified military command structure under a Secretary of Defense, and a National Security Council (NSC) to advise the President "with respect to the integration of domestic, foreign, and military policies relating to the national security."[4] The fundamental intent of this legislation was to coordinate U.S. national defense efforts, including intelligence activities, in the face of a Soviet Union intent upon expanding and leading a system of communist states.

In response to the rapid growth and changing role of the Federal government following the Second World War, several studies were conducted to examine the structure and efficiency of the executive branch, including the intelligence agencies.[5] Between 1948 and 1949, two important investigations of the national intelligence effort were conducted. The first, the Task Force on National Security Organization of the First Hoover Commission, was established by a unanimous vote in Congress. The second, known as the Dulles-Jackson-Correa Report, was initiated by the NSC at the request of President Harry S. Truman.

---

[3]Lewis Carroll, *Alice's Adventures in Wonderland* (New York: Barnes & Noble Books, 1994), p. 125.

[4]Section 101(a), National Security Act of 1947.

[5]For a comprehensive examination of similar Commissions see: Ronald C. Moe, *Reorganizing the Executive Branch in the Twentieth Century: Landmark Commissions*, CRS Report 92-293 GOV, March 19, 1992.

The First Hoover Commission, 1949

The Commission on Organization of the Executive Branch of the government was established pursuant to P.L. 80-162 of July 27, 1947.[6] Under the chairmanship of former President Herbert Hoover, the twelve man bipartisan commission conducted a comprehensive review of the federal bureaucracy, including the intelligence agencies. The commission's Task Force on National Security Organization was headed by Ferdinand Eberstadt, a strong advocate of a centralized intelligence capability who had been instrumental in drafting the National Security Act of 1947.[7]

Hearings conducted by the task force began in June 1948. On January 13, 1949, the Hoover Commission submitted the task force's 121 page unclassified report to Congress.[8] Known as the Eberstadt Report, it found the "National Security Organization, established by the National Security Act of 1947, [to be] soundly constructed, but not yet working well."[9] The report identified fundamental organizational and qualitative shortcomings in the national intelligence effort and the newly created CIA.

A principal concern of the task force was the adversarial relationship and lack of coordination between the CIA, the military, and the State Department. It suggested that this resulted in unnecessary duplication and the issuance of departmental intelligence estimates that "have often been subjective and biased."[10] In large measure, the military and State Department were blamed for their failure to consult and share pertinent information with the CIA. The task force recommended "that positive efforts be made to foster relations of mutual confidence between the [CIA] and the several departments and agencies that it serves."[11]

In short, the report stressed that the CIA "must be the central organization of the national intelligence system."[12] To facilitate community coordination in the production of national estimates, a founding intent of CIA, the task force recommended the creation within CIA "at the top echelon an evaluation board or section composed of competent and experienced personnel who would have no administrative responsibilities and whose duties would be

---

[6]The report was reprinted as *The Hoover Commission Report on Organization of the Executive Branch of the Government* (Westport, CT: Greenwood Press, 1970).

[7]For background on Eberstadt, see Jeffrey M. Dorwart, *Eberstadt and Forrestal: A National Security Partnership, 1909-1949* (College Station, TX: Texas A & M University Press, 1991).

[8]The Commission on Organization of the Executive Branch of the Government, *Task Force Report on National Security Organization*, Appendix G, January 1949; hereafter cited as the Eberstadt Report.

[9]Eberstadt Report, p. 3.

[10]Eberstadt Report, p. 76.

[11]Eberstadt Report, p. 16, paragraph d.

[12]Arthur B. Darling, *The Central Intelligence Agency: An Instrument of Government to 1950* (University Park, PA: Pennsylvania State University Press, 1990), p. 293. This is a reprint of an official CIA history prepared in the early 1950's.

confined solely to intelligence evaluation."[13] To foster professionalism and continuity of service, the report also favored a civilian DCI with a long term in office.[14]

In the arena of covert operations and clandestine intelligence, the Eberstadt Report supported the integration of all clandestine operations into one office within CIA, under NSC supervision. To alleviate concerns expressed by the military who viewed this proposal as encroaching upon their prerogatives, the report stated that clandestine operations should be the responsibility of the Joint Chiefs of Staff (JCS) in time of war.[15]

In examining the daily workings of the CIA, the task force found the agency's internal structure and personnel system "not now properly organized."[16] This led to recommendations for the adoption of clearer lines of departmental responsibilities, and the establishment of proper personnel selection and training systems.[17] In response to legislative concerns regarding intelligence budgets, the report supported establishing a legal framework for budgetary procedures and authorities, and in maintaining the secrecy of the CIA budget in order to provide the "administrative flexibility and anonymity that are essential to satisfactory intelligence."[18] The report also addressed, and rejected, the possibility of placing the FBI's counterintelligence responsibilities in the CIA.[19]

Of particular concern was the level of professionalism in military intelligence, and the glaring inadequacies of medical and scientific intelligence, including biological and chemical warfare, electronics, aerodynamics, guided missiles, atomic weapons, and nuclear energy.[20] The report declared that the failure to appraise scientific advances in hostile countries (*i.e.*, the Soviet Union) might have more immediate and catastrophic consequences than failure in any other field of intelligence. Accordingly, the report stressed that the U.S. should establish a central authority "to collect, collate, and evaluate scientific and medical intelligence."[21]

Intelligence Survey Group (Dulles-Jackson-Correa Report), 1949

---

[13]Eberstadt Report, p. 16.

[14]Darling, introduction to Chapter VIII.

[15]Darling, introduction to chapter VIII.

[16]Eberstadt Report, p. 76.

[17]Darling, pp. 295-298.

[18]Darling, p. 297.

[19]Darling, p. 289.

[20]Eberstadt Report, p. 77; Darling, p. 296.

[21]Eberstadt Report, p, 20.

On January 8, 1948, the National Security Council established the Intelligence Survey Group (ISG) to "evaluate the CIA's effort and its relationship with other agencies."[22] Commissioned at the request of President Truman, the group was composed of Allen W. Dulles, who had served in the Office of Strategic Services (OSS) during the Second World War and would become DCI in 1953, William Jackson, a future Deputy DCI, and Matthias Correa, a former assistant to Secretary of Defense James V. Forrestal when the latter had served as Secretary of the Navy during the war. Under the chairmanship of Dulles, the ISG presented its findings, known as the Dulles-Jackson-Correa Report, to the National Security Council on January 1, 1949.

The 193-page report, partially declassified in 1976, contained fifty-six recommendations, many highly critical of the CIA and DCI.[23] In particular, the report revealed problems in the agency's execution of both its intelligence and operational missions. It also criticized the quality of national intelligence estimates by highlighting the CIA's--and, by implication, the DCI's--"failure to take charge of the production of coordinated national estimates."[24] The report went on to argue that the CIA's current trend in secret intelligence activities should be reversed in favor of its mandated role as coordinator of intelligence.[25]

The Dulles Report was particularly concerned about the personnel situation at CIA, including internal security, the high turnover of employees, and the excessive number of military personnel assigned to the agency.[26] To add "continuity of service" and the "greatest assurance of independence of action," the report argued that the DCI should be a civilian and that military appointees be required to resign their commissions.[27]

As with the Eberstadt Report, the Dulles Report also expressed concern about the inadequacies in scientific intelligence and the professionalism of the service intelligence organizations, and urged that the CIA provide greater coordination.[28] This led to a recommendation for increased coordination between the DCI and the Director of the Federal Bureau of Investigation (FBI) in the arena of counterespionage. In turn, the report recommended that the Director of FBI be elevated to membership in the Intelligence Advisory

---

[22]Mark M. Lowenthal, *U.S. Intelligence: Evolution and Anatomy* (Westport, CT: Praeger, 1992), p. 20.

[23]"The Central Intelligence Agency and National Organization for Intelligence: A Report to the National Security Council," January 1, 1949. Hereafter cited as the Dulles-Jackson-Correa Report; the declassified report remains highly sanitized. A version was reprinted in William M. Leary, ed., *The Central Intelligence Agency: History and Documents* (University, AL: University of Alabama Press, 1984).

[24]Lowenthal, p. 20; Dulles-Jackson-Correa Report, p. 5, 11.

[25]Dulles-Jackson-Correa Report, p. 39.

[26]DCI Hillenkoetter disputed these findings by producing evidence that CIA's employee turnover was no different than in other government agencies and that only two percent of CIA personnel were active duty military. Darling, p. 327.

[27]Dulles-Jackson-Correa Report, p. 138.

[28]Dulles-Jackson-Correa Report, pp. 3-4, 149.

Committee (IAC), whose function was to help the DCI coordinate intelligence and set intelligence requirements.[29]

The principal thrust of the report was a proposed large-scale reorganization of the CIA to end overlapping and duplication of functions. Similar to the Eberstadt Report, the Dulles study suggested incorporating covert operations and clandestine intelligence into one office within CIA. In particular, the report recommended that the Office of Special Operations (OSO), responsible for the clandestine collection of intelligence, and the Office of Policy Coordination (OPC), responsible for covert actions, be integrated into a single division within CIA.[30]

Accordingly, the report recommended replacing existing offices with four new divisions for coordination, estimates, research and reports, and operations. The heads of the new offices would be included in the immediate staff of the DCI so that he would have "intimate contact with the day-to-day operations of his agency and be able to give policy guidance to them."[31] These recommendations would become the blueprint for the future organization and operation of the present-day CIA.

Summary of the Truman Administration Intelligence Investigations

The Task Force on National Security Organization was almost immediately eclipsed by the Dulles-Jackson-Correa Report, that found a sympathetic ear in the White House. On July 7, 1949, the NSC adopted a modified version of the Dulles Report, and directed DCI Roscoe H. Hillenkoetter to begin implementing its recommendations, including the establishment of a single operations division at CIA. In 1953, the OSO and OPC were merged within the CIA to form the Directorate of Plans (DP). (DP was designated the Directorate of Operations (DO) in 1973.)

Although the Eberstadt Report was not as widely read among policymakers as the Dulles study, it did play a principal role in reorganization efforts initiated by DCI Walter Bedell Smith in 1950. The two reports, and the lessons learned from fall of China to the Communists and the unexpected North Korean invasion of South Korea in June 1950, prompted Smith to create an intelligence evaluation board called the Board of National Estimates (BNE). Designed to review and produce National Intelligence Estimates (NIEs), the BNE was assisted by an Office of National Estimates (ONE) that drew upon the resources of the entire community.[32]

The Eisenhower Administration, 1953-1961

---

[29]Dulles-Jackson-Correa Report, p. 58. Although the DCI served as chairman of the IAC, he was not given budgetary or administrative authority over the other intelligence agencies.

[30]Dulles-Jackson-Correa Report, pp. 129, 134.

[31]Dulles-Jackson-Correa Report, p. 11.

[32]The work of the BNE is described in Donald P. Steury, ed., *Sherman Kent and the Board of National Estimates: Collected Essays* (Washington: Center for the Study of Intelligence, 1994).

The Eisenhower Administration witnessed the Soviet Union solidify its hold over Eastern Europe, crushing the Hungarian revolution, and the rise of Communist insurgencies in Southeast Asia and Africa. This was a period in which extensive covert psychological, political, and paramilitary operations were initiated in the context of the threat posed by Soviet-led Communist expansion. However, between 1948, when a covert action program was first authorized through NSC Directive 10/2, and 1955 there was no formally established procedure for approval.

Between 1954 and 1956, this prompted three investigations into U.S. intelligence activities, including the CIA. The first, the Task Force on Intelligence Activities of the Second Hoover Commission on Organization of the Executive Branch of the Government, was sponsored by Congress. The second, the Doolittle Report, was commissioned at the request of President Dwight D. Eisenhower in response to the Second Hoover Commission. The third, the Bruce-Lovett Report was initiated by the President's Board of Consultants on Foreign Intelligence Activities (PBCFIA), and reported to President Eisenhower.

Second Hoover Commission, 1955

The Commission on Organization of the Executive Branch of the Government, also chaired by former President Hoover, was created pursuant to P.L. 83-108 of July 10, 1953. Known as the Second Hoover Commission, it contained a Task Force on Intelligence Activities under the chairmanship of General Mark W. Clark. In May 1955, the task force submitted both classified and unclassified reports. The classified version was sent directly to President Eisenhower, and has not been declassified according to available information. The unclassified version was sent to Congress.

The unclassified report's seventy-six pages contained nine recommendations and briefly described the evolution of the Intelligence Community and its then-current functioning. The report initiated the official use of the term "Intelligence Community."[33] Until that time, the U.S. had sought to apply increasing coordination to departmental intelligence efforts, without the concept of a "community" of departments and agencies.

The task force began by expressing the need to reform the CIA's internal organization, including the recommendation that the DCI concentrate on intelligence issues facing the entire community by leaving the day-to-day administration of the CIA to an executive officer or chief of staff.[34] It foresaw the need for better oversight of intelligence activities and proposed a small, permanent, bipartisan commission, including Members of Congress and other "public-spirited citizens," to provide independent oversight of intelligence activities that were normally kept secret from other parts of the government.[35] The full commission's report elaborated

---

[33]Commission on Organization of the Executive Branch of the Government, A Report to the Congress, *Intelligence Activities*, June 1955, p. 13; hereafter cited as Clark Task Force Report.

[34]Clark Task Force Report, pp. 70-71. For a more detailed account of the evolution of the DCI's roles and responsibilities, see Herbert Andrew Boerstling, "The Establishment of a Director of National Intelligence," unpublished Master of Arts Policy Paper, Boston University, August 1995.

[35]Clark Task Force Report, p. 71.

on this by recommending the establishment of both a congressional oversight committee and a presidential advisory panel.

The task force also expressed concern about counterintelligence and recommended systematic rechecking of all personnel every five years "to make sure that the passage of time has not altered the trustworthiness of any employee, and to make certain that none has succumbed to some weakness of intoxicants or sexual perversion."[36]

In addition, the task force recommended that the CIA replace the State Department in the "procurement of foreign publications and for collection of scientific intelligence."[37] Finally, there were a number of "housekeeping" recommendations such as the need to construct an adequate CIA headquarters, to improve linguistic training, and to raise the salary of the DCI to $20,000 annually.[38]

The Doolittle Report, 1954

In response to the establishment of the Second Hoover Commission's Task Force on Intelligence Activities, President Eisenhower sought and secured an agreement for a separate report to be presented to him personally on the CIA's Directorate of Plans, that now had responsibility for both clandestine intelligence collection and covert operations. Accordingly, in July 1954, Eisenhower commissioned Lieutenant General James Doolittle (USAF) to report on the CIA's covert activities and to "make any recommendations calculated to improve the conduct of these operations."[39]

On September 30, 1954, Doolittle submitted his 69-page classified report directly to Eisenhower. Declassified in 1976, the Doolittle Report contained forty-two recommendations. The report began by summarizing contemporary American Cold War attitudes following the Korean War:

> It is now clear that we are facing an implacable enemy whose avowed objective is world domination by whatever means and at whatever cost. There are no rules in such a game...If the United States is to survive, long-standing American concepts of "fair play" must be reconsidered. We must develop effective espionage and counterespionage services and must learn to subvert, sabotage and destroy our enemies by more clever, more sophisticated and more effective methods than those used against us. It may become necessary that the American people be made acquainted with, understand and support this fundamentally repugnant philosophy.[40]

---

[36]Clark Task Force Report, p. 74.

[37]Clark Task Force Report, p. 74.

[38]Clark Task Force Report, pp. 72-76.

[39]*The Report on the Covert Activities of the Central Intelligence Agency*, September 30, 1954, Appendix A, p. 54; hereafter cited as the Doolittle Report.

[40]Doolittle Report, pp. 6-7.

The report went on to recommend that "every possible scientific and technical approach to the intelligence problem" be explored since the closed society of the Eastern Bloc made human espionage "prohibitive" in terms of "dollars and human lives."[41]

In examining the CIA, Doolittle found it to be properly placed in the organization of the government. Furthermore, the report found the laws relating to the CIA's functions were sufficient for the agency to meet its operational needs, *i.e.* penetration of the Soviet Bloc.[42] The report went on to issue several recommendations calling for more efficient internal administration, including recruitment and training procedures, background checks of personnel, and the need to "correct the natural tendency to over classify documents originating in the agency."[43] It also called for increased cooperation between the clandestine and analytical sides of the agency, and recommended that the "Inspector General ... operate on an Agency-wide basis with authority and responsibility to investigate and report on all activities of the Agency."[44] Finally, the report mentioned the need to provide CIA with accommodations tailored to its specific needs, and to exercise better control (accountability) of expenditures in covert projects.

Shortly after submitting the written report, General Doolittle voiced his concern to President Eisenhower over the potential difficulties that could arise from the fact that the DCI, Allen Dulles, and the Secretary of State, John Foster Dulles, were brothers and might implement policies without adequate consultation with other administration officials.[45]

Bruce-Lovett Report, 1956

In 1956, PBCFIA's chairman, James Killian, president of the Massachusetts Institute of Technology, directed David Bruce, a widely experienced diplomat, and Robert Lovett, a prominent attorney, to prepare a report for President Eisenhower on the CIA's covert action programs as implemented by NSC Directive 10/2. The report itself has not been located by either the CIA's Center for the Study of Intelligence or by private researchers. Presumably, it remains classified. However, Peter Grose, biographer of Allen Dulles, was able to use notes of the report prepared years earlier by historian Arthur M. Schlesinger, Jr.[46]

---

[41]Doolittle Report, pp. 7-8.

[42]Doolittle Report, p. 10.

[43]Doolittle Report, p. 14.

[44]Doolittle Report, p. 17.

[45]John Ranelagh, *The Agency: the Rise and Decline of the CIA* (New York: Simon and Schuster, 1987), p. 278.

[46]Peter Grose, *Gentleman Spy: The Life of Allen Dulles*, (Boston: Houghton Mifflin, 1994), pp. 445-448; also the CIA's Center for the Study of Intelligence *Newsletter*, Spring 1995, Issue No. 3, pp. 3-4. In writing this book, Grose reported using notes Arthur M. Schlesinger, Jr. discovered in the Robert Kennedy Papers before they were deposited at the John F. Kennedy Library; p. 598, n. 33 and n. 34. Reportedly, the JFK Presidential Library has unsuccessfully searched the RFK papers for the report.

According to Grose's account of the Schlesinger notes, the report criticized the CIA for being too heavily involved in Third-World intrigues while neglecting the collection of hard intelligence on the Soviet Union. Reportedly, Bruce and Lovett went on to express concern about the lack of coordination and accountability of the government's psychological and political warfare program. Stating that "no charge is made for failure," the report claimed that "No one, other than those in CIA immediately concerned with their day-to-day operation, has any detailed knowledge of what is going on."[47] These operations, asserted Bruce and Lovett, were in the hands of a "horde of CIA representatives (largely under State or Defense cover),...bright, highly graded young men who must be doing something all the time to justify their reason for being."[48]

As had Doolittle, Bruce and Lovett criticized the close relationship between Secretary of State John Foster Dulles and his brother DCI Allen W. Dulles. Due to the unique position of each brother, the report apparently expressed concern that they could unduly influence U.S. foreign policy according to their own perceptions.[49]

The report concluded by suggesting that the U.S. reassess its approach to covert action programs, and that a permanent authoritative position be created to assess the viability and impact of covert action programs.[50]

Summary of the Eisenhower Administration Intelligence Investigations

As a result of the Second Hoover Commission's Report and General Doolittle's findings, two new NSC Directives, 5412/1 and 5412/2, were issued pertaining to covert activities in March and November 1955, respectively. Together, these directives instituted control procedures for covert action and clandestine activities. They remained in effect until 1970, providing basic policy guidelines for the CIA's covert action operations.

In 1956, in response to the Clark Task Force, and to preempt closer congressional scrutiny of intelligence gathering, President Eisenhower created the President's Board of Consultants on Foreign Intelligence Activities (PBCFIA) to conduct independent evaluations of the U.S. intelligence program. PBCFIA became the President's Foreign Intelligence Advisory Board (PFIAB) in 1961. Permanent intelligence oversight committees were not established in Congress until the mid-1970s.

When the Bruce-Lovett Report was first issued in the autumn of 1956, its immediate impact was muted due to the contemporaneous Suez Canal crisis and the Soviet invasion of Hungary. However, it did establish a precedent for future PBCFIA investigations into intelligence activities.

---

[47]Grose, p. 446; from excerpts of the Schlesinger notes.

[48]Grose, p. 446; this observation is also taken from excerpts of the Schlesinger notes.

[49]Grose, p. 447.

[50]Grose, pp. 447-448; from excerpts of the Schlesinger notes.

The Kennedy Administration, 1961-1963

In the 1950s, the Eisenhower Administration had supported covert CIA initiatives in Iran (1953) and Guatemala (1954) to overthrow governments unfriendly to the United States. These operations were planned to provide the United States with a reasonable degree of plausible deniability. During the last Eisenhower years, revolution in Cuba resulted in a Communist government under Fidel Castro. In the context of the Cold War, a communist Cuba appeared to justify covert U.S. action to secure a change in that nation's government. In April 1961 an ill-fated U.S. backed invasion of Cuba led to a new chapter in the history of the Intelligence Community.

On April 17, 1961, some 1,400 Cuban exiles of the Cuban Expeditionary Force (CEF), trained and supported by the CIA, landed at the Bay of Pigs in Cuba with the hope of overthrowing the communist regime of Fidel Castro. Known as Operation Zapata, the invasion was a complete disaster. Over the first two days, Castro succeeded in defeating the invasion force and exposing direct U.S. involvement.

The fiasco led to two official examinations of U.S. involvement and conduct in Operation Zapata. The first, the Taylor Commission, was initiated by President John F. Kennedy in an attempt to ascertain the overall cause of the operation's failure. The second, the Kirkpatrick Report, was an internal CIA investigation to determine what had been done wrong.

The Taylor Commission

On April 22, President Kennedy asked General Maxwell Taylor, former Army Chief of Staff, to chair a high-level body composed of Attorney General Robert Kennedy, former Chief of Naval Operations Admiral Arleigh Burke, and DCI Allen Dulles to ascertain the reasons for the invasion's failure. Known as the Taylor Commission, the study group's 53-page classified report was submitted to President Kennedy on June 13, 1961.

Declassified in 1977, the report examined the conception, development, and implementation of Operation Zapata. The commission's final report focused on administrative rather than operational matters, and evenly leveled criticism at the White House, the CIA, the State Department, and the Joint Chiefs of Staff.[51]

The report found that the CIA, at White House direction, had organized and trained Cuban exiles to enter Cuba, foment anti-Castro sentiment, and ultimately overthrow the Cuban government. Originally intended by the Eisenhower Administration as a guerrilla operation, Zapata was supposed to operate within the parameters of NSC Directive 5412/2, that called in part for plausible U.S. deniability. However, in the Kennedy Administration, the operation grew in size and scope to include a full-scale military invasion involving "sheep-dipped" B-26 bombers, supply ships and landing craft.[52] The report found that "the magnitude of Zapata

---

[51] Grose, p. 532.

[52] "Sheep-dipped" is a colloquial intelligence term used for administrative arrangements designed to insure that the origin of a person or object is non-traceable.

could not be prepared and conducted in such a way that all U.S. support of it and connection with it could be plausibly disclaimed."[53]

In large measure, the report blamed the operation's planners at the CIA's Directorate of Plans for not keeping the President fully informed as to the exact nature of the operation. However, the report also criticized the State Department, JCS, and the White House for acquiescing in the Zapata Plan, that "gave the impression to others of approving it" and for reviewing "successive changes of the plan piecemeal and only within a limited context, a procedure that was inadequate for a proper examination of all the military ramifications."[54]

The Taylor Commission found the operation to be ill-conceived with little chance for ultimate success. Once underway, however, the report cited President Kennedy's decision to limit overt U.S. air support as a factor in the CEF's defeat.[55] This decision was apparently reached in order to protect the covert character of the operation. The report criticized this decision by stating that when an operation had been approved, "restrictions designed to protect its covert character should have been accepted only if they did not impair the chance of success."[56]

The failure in communication, breakdown in coordination, and lack of overall planning led the Taylor Commission to conclude that:

> The Executive Branch of government was not organizationally prepared to cope with this kind of paramilitary operation. There was no single authority short of the President capable of coordinating the actions of CIA, State, Defense and USIA [U.S. Information Agency]. Top level direction was given through *ad hoc* meetings of senior officials without consideration of operational plans in writing and with no arrangement for recording conclusions reached.[57]

The lessons of Operation Zapata led the report to recommend six courses of action in the fields of planning, coordination, effectiveness, and responsibility in overall Cold War strategy. The report recommended the creation of a Strategic Resources Group (SRG) composed of representatives of under-secretarial rank from the CIA and the Departments of State and Defense. With direct access to the President, the SRG would act as a mechanism for the planning and coordination of overall Cold War strategy, including paramilitary operations. The report recommended including the opinions of the JCS in the planning and implementation of such paramilitary operations. In the context of the Cold War, the report also recommended a review of restraints placed upon the United States in order to make the

---

[53]The report was published as *Operation Zapata: The "Ultrasensitive" Report and Testimony of the Board of Inquiry on the Bay of Pigs* (Frederick, MD: University publications of America, Inc., 1981), p. 40; hereafter cited as the Taylor Report.

[54]Taylor Report, p. 43.

[55]Taylor Report, p. 38.

[56]Taylor Report, p. 40.

[57]Taylor Report, p. 39.

most effective use of the nation's assets, without concern for international popularity. The report concluded by reaffirming America's commitment to forcing Castro from power.[58]

The Kirkpatrick Report

Concurrent with the Taylor Commission, DCI Dulles instructed the CIA's Inspector General, Lyman B. Kirkpatrick, Jr., to conduct an internal investigation to determine what the CIA had done wrong in the Cuban operation. Completed in five months, the report was viewed by the few within CIA who read it as professionally shabby.[59] Whereas the Taylor Report had more of the detached perspective of a management-consultant, the Kirkpatrick Report was viewed as a personal attack against the CIA and DCI Dulles.

The 170-page report remains classified. However, in 1972, Kirkpatrick published an article in the *Naval War College Review* that apparently reflected the findings of his report.[60] In particular, Kirkpatrick criticized the Zapata planners at the Directorate of Plans for not having fully consulted the CIA's Cuban analysts before the invasion. The article also criticized the operation's internal security, that Kirkpatrick claimed was virtually nonexistent. Calling the operation frenzied, Kirkpatrick accused the CIA of "playing it by ear" and misleading the President by failing to inform him that "success had become dubious."[61] In Kirkpatrick's view, the CIA bore most of the blame, and the Kennedy Administration could be forgiven for having trusted the advice of the operation's planners at the Agency.

Summary of the Kennedy Administration Intelligence Investigations

On May 4, 1961, following the Bay of Pigs, President Kennedy reconstituted the PBCFIA as the President's Foreign Intelligence Advisory Board (PFIAB). Although little is known of the Kirkpatrick Report's impact, the Taylor Report influenced Kennedy's desire to improve the overall management of the intelligence process. In 1962, this prompted the President to instruct the new DCI, John McCone, to concentrate on his community-wide coordination role:

> As [DCI], while you will continue to have overall responsibility for the Agency, I shall expect you to delegate to your principal deputy, as you may deem necessary,

---

[58]Taylor Report, pp. 44-53.

[59]Ranelagh, p. 380.

[60]Lyman B. Kirkpatrick, Jr., "Paramilitary Case Study - Bay of Pigs," *Naval War College Review*, (November-December 1972). By the same author, see *The U.S. Intelligence Community: Foreign Policy and Domestic Activities* (New York: Hill and Wang, 1973).

[61]Evan Thomas, *The Very Best Men, Four Who Dared: The Early Years of the CIA*, (New York: Simon & Schuster, 1995), p. 268. Thomas was given special permission to review the report for use in his book even though it remains classified.

so much of the detailed operation of the Agency as may be required to permit you to carry out your primary task as [DCI].[62]

The Johnson Administration, 1963-1969

No major investigations of the Intelligence Community were conducted under President Lyndon B. Johnson. In large measure, this was due to America's growing preoccupation with the Vietnam conflict and the strain that this placed on the community's resources. The only major investigation during the Johnson Administration was the Warren Commission on the assassination of President Kennedy. Former DCI Allen Dulles served on the commission.

The Nixon Administration, 1969-1974

During the Vietnam War, the Intelligence Community devoted enormous attention in both manpower and resources towards achieving U.S. policy objectives in Southeast Asia. As the U.S. effort in Vietnam and Laos wound down, and attention turned towards strategic weapons concerns with the Soviet Union, some members of the Nixon Administration believed that the community was performing less than adequately. In 1970, President Richard M. Nixon and National Security Advisor Henry A. Kissinger undertook a review of the Intelligence Community's organization.

The Schlesinger Report, 1971

In December 1970, President Nixon commissioned the Office of Management and Budget (OMB) to examine the Intelligence Community's organization and recommend improvements, short of legislation. In March 1971, the report, "A Review of the Intelligence Community," was submitted by Deputy OMB Director James R. Schlesinger, a future DCI.

Known as the Schlesinger Report, the study's forty-seven pages noted the community's "impressive rise in...size and cost" with the "apparent inability to achieve a commensurate improvement in the scope and overall quality of intelligence products."[63] The report sought to uncover the causes of this problem and identify areas in which constructive change could take place.

In examining the Intelligence Community, Schlesinger criticized "unproductively duplicative" collection systems and the failure in forward planning to coordinate the allocation of resources.[64] In part, the report cited the failure of policymakers to specify their product needs to the intelligence producers.[65] However, the report identified the primary cause of

---

[62]Memorandum for the Director of Central Intelligence, January 16, 1962; quoted in Prados, 89-414F, p. 45.

[63]*A Review of the Intelligence Community*, March 10, 1971, p. 1; hereafter cited as the Schlesinger Report.

[64]Schlesinger Report, pp. 8-9.

[65]Schlesinger Report, p. 9.

these problems as the lack of a strong, central Intelligence Community leadership that could "consider the relationship between cost and substantive output from a national perspective."[66] Schlesinger found that this had engendered a fragmented, departmental intelligence effort.

To correct these problems, Schlesinger considered the creation of a Director of National Intelligence (DNI), enhancing the DCI's authority, and establishing a Coordinator of National Intelligence (CNI) who would act as the White House-level overseer of the Intelligence Community to provide more direct representation of presidential interest in intelligence issues.[67] In the end, the report recommended "a strong DCI who could bring intelligence costs under control and intelligence production to an adequate level of quality and responsiveness."[68]

Summary of the Nixon Administration Intelligence Investigation

The Schlesinger Report led to a limited reorganization of the Intelligence Community under a Presidential directive dated November 5, 1971. In part, the directive called for:

> An enhanced leadership role for the [DCI] in planning, reviewing, and evaluating all intelligence programs and activities, and in the production of national intelligence.[69]

Consequently, two boards were established to assist the DCI in preparing a consolidated intelligence budget and to supervise community-wide intelligence production. The first, was the ill-fated Intelligence Resources Advisory Committee (IRAC), that replaced the National Intelligence Resources Board (NIRB) established in 1968 under DCI Richard Helms. The IRAC was designed to advise the DCI on the preparation of a consolidated budget for the community's intelligence programs. However, IRAC was not afforded the statutory authority necessary to bring the intelligence budget firmly under DCI control. The second, and the only long lasting result of the Nixon directive, was the establishment of the Intelligence Community Staff (ICS) in 1972. Created by DCI Helms, the ICS was meant to assist the DCI in guiding the community's collection and production of intelligence. However, the ICS did not provide the DCI with the statutory basis necessary for an expanded community-wide role.[70] In 1992, DCI Robert Gates replaced the ICS with the Community Management Staff (CMS).

The Era of Public Investigations, 1974-1981

---

[66]Schlesinger Report, p. 13.

[67]Schlesinger Report, pp. 25-33.

[68]U.S. Congress, Senate, 94th Congress, 2nd session, Select Committee to Study Governmental Operations with Respect to Intelligence Activities Intelligence, *Final Report*, 1976, Book I, p. 66; hereafter cited as the Church Committee Report.

[69]"Reorganization of the U.S. Intelligence Community," *Weekly Compilation of Presidential Documents*, November 4, 1971, pp. 1467-1491, 1482.

[70]Prados, 89-414F, p. 46.

In the late 1940s and throughout the 1950s, there had been widespread public agreement on the need for an effective national security structure to confront Soviet-led Communist expansion. However, by the late 1960s, the war in Vietnam had begun to erode public consensus and support for U.S. foreign policy. The controversy surrounding the Watergate Investigations after 1972, and subsequent revelations of questionable CIA activities involving domestic surveillance, provided a backdrop for increasing scrutiny of government policies, particularly in such fields as national security and intelligence.

Between 1975 and 1976, this led the Ford Administration and Congress to conduct three separate investigations that examined the propriety of intelligence operations, assessed the adequacy of intelligence organizations and functions, and recommended corrective measures. A fourth panel, convened earlier to look more broadly at foreign policy, also submitted recommendations for intelligence reform.

Murphy Commission, (Commission on the Organization of the Government for the Conduct of Foreign Policy), 1975

The Commission on the Organization of the Government for the Conduct of Foreign Policy, created pursuant to the Foreign Relations Authorization Act for FY1973 (P.L. 92-352) of July 13, 1972, was headed by former Deputy Secretary of State Robert D. Murphy. It looked at national security formulation and implementation processes rather than the government as a whole. As such, the Murphy Commission was more focused than either of the two Hoover Commissions and devoted greater attention to intelligence issues. Although it made reference to the need to correct "occasional failures to observe those standards of conduct that should distinguish the behavior of agencies of the U.S. Government,"[71] the commission's approach was marked by an emphasis of the value of intelligence to national security policymaking and was, on the whole, supportive of the Intelligence Community.

Many of the Murphy Commission's recommendations addressed problems that have continued to concern successive intelligence managers. The commission noted the fundamental difficulty that DCIs have line authority over the CIA but "only limited influence" over other intelligence agencies.[72] Unlike other observers, the Murphy Commission did not believe that this situation should be changed fundamentally: "[It] is neither possible nor desirable to give the DCI line authority over that very large fraction of the intelligence community that lies outside the CIA." At the same time, it recommended that the DCI have an office in close proximity to the White House and be accorded regular and direct contact with the President. The commission envisioned a DCI delegating considerable authority for managing the CIA to a deputy while he devoted more time to community-wide responsibilities. The commission also recommended that the DCI's title be changed to Director of Foreign Intelligence.[73]

The commission provided for other oversight mechanisms, *viz.*, a strengthened PFIAB and more extensive review (prior to their initiation and on a continuing basis thereafter) of

---

[71]U.S., Commission on the Organization of the Government for the Conduct of Foreign Policy, *Report*, June 1975, p. 92.

[72]Commission on Organization of the Government, p. 98

[73]Commission on Organization of the Government, pp. 98-99.

covert actions by a high-level interagency committee. It argued that although Congress should be notified of covert actions, the President should not sign such notifications since it is harmful to associate "the head of State so formally with such activities.[74]" It was further recommended that intelligence requirements and capabilities be established at the NSC-level to remedy a situation in which "the work of the intelligence community becomes largely responsive to its own perceptions of what is important, and irrelevant information is collected, sometimes drowning out the important.[75]" It also recommended that this process be formalized in an officially approved five-year plan. A consolidated foreign intelligence budget should also be prepared, approved by an inter-agency committee and OMB and submitted to Congress.

Although the importance of economic intelligence was recognized, the commission did not see a need for intelligence agencies to seek to expand in this area; rather, it suggested that the analytical capabilities of the Departments of State, Treasury, Commerce, Agriculture, and the Council of Economic Advisers should be significantly strengthened.

The commission noted the replacement of the Board of National Estimates by some eleven National Intelligence Officers (NIOs) who were to draw upon analysts in various agencies to draft National Intelligence Estimates (NIEs). This practice was criticized because it laid excessive burdens on chosen analysts and because NIEs had in recent years been largely ignored by senior officials (presumably Secretary of State Kissinger) who made their own assessments of future developments based on competing sources of information and analysis. Thus, the commission recommended a small staff of analysts from various agencies assigned to work with NIOs in drafting NIEs and ensure that differences of view were clearly presented for the policymakers.

Rockefeller Commission (Commission on CIA Activities within the United States), 1975

Prior to the mid-1960s, the organization and activities of the Intelligence Community were primarily the concern of specialists in national security and governmental organization. The Murphy Commission, although working during a subsequent and more politically turbulent period, had approached intelligence reorganization from this perspective as well. The political terrain had, however, been shifting dramatically and the Intelligence Community would not escape searching criticism. During the era of the Vietnam War and Watergate, disputes over national security policy focused attention on intelligence activities. In 1975, media accounts of alleged intelligence abuses, some stretching back over decades led to a series of highly publicized congressional hearings.

Revelations of assassination plots and other alleged abuses spurred three separate investigations and sets of recommendations. The first was undertaken within the Executive Branch and was headed by Vice President Nelson A. Rockefeller. Other investigations were conducted by select committees in both houses of Congress. The Senate effort was led by Senator Frank Church and the House committee was chaired by Representative Otis Pike. These investigations led to the creation of the two permanent intelligence committees and

---

[74]Commission on Organization of the Government, pp. 100-101.

[75]Commission on Organization of the Government, p. 101.

much closer oversight by the Congress. In addition, they also produced a number of recommendations for reorganization and realignment within the Intelligence Community.

Established by Executive Order 11828 on January 4, 1975, the Commission on CIA Activities within the United States was chaired by Vice President Rockefeller and included seven others appointed by President Ford (including then-former Governor Ronald Reagan). The commission's mandate was to investigate whether the CIA had violated provisions of the National Security Act of 1947, precluding the CIA from exercising internal security functions.

The Rockefeller Commission's 30 recommendations[76] included a number of proposals designed to delimit CIA's authority to collect foreign intelligence within the United States (from "willing sources") and proscribe collection of information about the domestic activities of U.S. citizens, to strengthen PFIAB, to establish a congressional joint intelligence committee, and to establish guidelines for cooperation with the Justice Department regarding the prosecution of criminal violations by CIA employees. There was another recommendation to consider the question of whether the CIA budget should be made public, if not in full at least in part.

The commission recommended that consideration should be given to appointing DCIs from outside the career service of the CIA and that no DCI serve longer than 10 years. Two deputies should be appointed; one to serve as an administrative officer to free the DCI from day-to-day management duties; the other a military officer to foster relations with the military and provide technical expertise on military intelligence requirements.

The CIA position of Inspector General should be upgraded and his responsibilities expanded along with those of the General Counsel. Guidelines should be developed to advise agency personnel as to what activities are permitted and what are forbidden by law and executive orders.

The President should instruct the DCI that domestic mail openings should not be undertaken except in time of war and that mail cover operations (examining and copying of envelopes only) are to be undertaken only on a limited basis "clearly involving matters of national security."

The commission was specifically concerned with CIA infiltration of domestic organizations and submitted a number of recommendations in this area. Presidents should refrain from directing the CIA to perform what are essentially internal security tasks and the CIA should resist any effort to involve itself in improper activities. The CIA "should guard against allowing any component ... to become so self-contained and isolated from top leadership that regular supervision and review are lost." Files of previous improper investigations should be destroyed. The agency should not infiltrate American organizations without a written determination by the DCI that there is a threat to agency operations, facilities, or personnel that cannot be met by law enforcement agencies. Other recommendations were directed at CIA investigations of its personnel or former personnel, including provisions relating to physical surveillance, wire or oral communications, and access to income tax information.

---

[76] *Report to the President by the Commission on CIA Activities Within the United States*, June 1975.

As a result of efforts by some White House staff during the Nixon Administration to use CIA resources improperly, a number of recommendations dealt with the need to establish appropriate channels between the agency and the Executive Office of the President.

Reacting to evidence that drugs had been tested on unsuspecting persons, the commission recommended that the practice should not be renewed. Also, equipment for monitoring communications should not be tested on unsuspecting persons within the United States. An independent agency should be established to oversee civilian uses of aerial photography to avoid any concerns over the improper domestic use of a CIA-developed system.

Concerned with distinguishing the separate responsibilities of the CIA and the Federal Bureau of Investigation (FBI), the commission urged that the DCI and the Director of the FBI prepare and submit to the National Security Council a detailed agreement setting forth the jurisdictions of each agency and providing for effective liaison between them.

The commission also recommended that all intelligence agencies review their holdings of classified information and declassify as much as possible.

Church Committee (Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities), 1976

Established in the wake of sensational revelations about assassination plots organized by the CIA, the Church Committee had a much wider mandate than the Rockefeller Commission, extending beyond the CIA to all intelligence agencies.[77] It too, however, concentrated on illegalities and improprieties rather than organizational or managerial questions *per se*. After extensive and highly publicized hearings, the committee made some 183 recommendations in its final report, issued April 26, 1976.[78]

The principal recommendation was that omnibus legislation be enacted to set forth the basic purposes of national intelligence activities and defining the relationship between intelligence activities and the Congress. Criticizing vagueness in the National Security Act of 1947, the committee urged charters for the several intelligence agencies to set forth general organizational structures and procedures, and delineate roles and responsibilities. There should also be specific and clearly defined prohibitions or limitations on intelligence activities. The effort to pass such legislation would consume considerable attention over a number of years, following the completion of the work of the Church Committee.

A number of recommendations reflected the committee's views on the appropriate role of the National Security Council in directing and monitoring the work of the intelligence agencies. The apparent goal was to encourage a more formal process, with accountability assigned to cabinet-level officials. The committee concluded that covert actions should be

---

[77]The definitive account of the Church Committee's work is Loch K. Johnson, *A Season of Inquiry: Congress and Intelligence*, 2nd. ed. (Chicago: Dorsey Press, 1988).

[78]U.S. Congress, Senate, 94th Congress, 2nd session, Select Committee to Study Governmental Operations with respect to Intelligence Activities, Foreign and Military Intelligence, *Final Report*, Book I, S. Rept. 94-755, April 26, 1976; hereafter cited as the Church Committee Report.

conducted only upon presidential authorization with notification to appropriate congressional committees.

Attention was given to the role of the DCI within the entire Intelligence Community. The committee recommended that the DCI be recognized by statute as the President's principal foreign intelligence advisor and that he should be responsible for establishing national intelligence requirements, preparing the national intelligence budget, and for providing guidance for intelligence operations.

The DCI should have specific responsibility for choosing among the programs of the different collection and production agencies and departments and to insure against waste and unnecessary duplication. The DCI should also have responsibility for issuing fiscal guidance for the allocation of all national intelligence resources. The authority of the DCI to reprogram funds within the intelligence budget should be defined by statute.[79]

Monies for the national intelligence budget would be appropriated to the DCI rather than to the directors of the various agencies. The committee also recommended that the DCI be authorized to establish an intelligence community staff to assist him in carrying out his managerial responsibilities. The staff should be drawn "from the best available talent within and outside the intelligence community."[80] Further, the position of Deputy DCI for the Intelligence Community should be established by statute (in addition to the existing DDCI who would have responsibility primarily for the CIA itself). It also urged consideration of separating the DCI from direct responsibility over the CIA.

The DCI, it was urged, should serve at the pleasure of the President, but for no more than ten years.

The committee also looked at intelligence analysis. It recommended a more flexible and less hierarchical personnel system with more established analysts being brought in at middle and upper grades. Senior positions should be established on the basis of analytical ability rather than administrative responsibilities. Analysts should be encouraged to accept temporary assignments at other agencies or on the NSC staff to give them an appreciation for policymakers' use of intelligence information. A system should be in place to ensure that analysts are more promptly informed about U.S. policies and programs affecting their areas of responsibility.

In addressing covert actions, the committee recommended barring political assassinations, efforts to subvert democratic governments, and support for police and other internal security forces engaged in systematic violations of human rights.

The committee addressed the questions of separating CIA's analysis and production functions from clandestine collection and covert action functions. It listed the pros and cons of this approach, but ultimately recommended only that the intelligence committees should give it consideration.

---

[79]Church Committee Report, pp. 434-435.

[80]Church Committee Report, p. 435.

Reflecting concerns about abuses of the rights of U.S. citizens, the committee made a series of recommendations regarding CIA involvement with the academic community, members of religious organizations, journalists, recipients of government grants, and the covert use of books and publishing houses. A particular concern was limiting any influence on domestic politics of materials published by the CIA overseas. Attention was also given to proprietary organizations CIA creates to conduct operations abroad; the committee believed them necessary, but advocated stricter regulation and congressional oversight.

The committee recommended enhanced positions for CIA's Inspector General (IG) and General Counsel (GC), urging that the latter be made a presidential appointee requiring Senate confirmation.

In looking at intelligence agencies other than the CIA, the committee recommended that the Defense Intelligence Agency (DIA) be made part of the civilian Office of the Secretary of Defense and that a small J-2 staff provide intelligence support to the Joint Chiefs of Staff. It was urged that the directors of both DIA and the National Security Agency (NSA) should be appointed by the President and confirmed by the Senate. The committee believe that either the director or deputy director of DIA and of NSA should be civilians. Turning to the State Department, the committee urged the Administration to issue instructions to implement legislation that authorized ambassadors to be provided information about activities conducted by intelligence agencies in their assigned countries. It also stated that State Department efforts to collect foreign political and economic information overtly should be improved.

Funding for intelligence activities has been included in Defense Department authorization and appropriations legislation since the end of World War II. The Church Commission advocated making public, at least, total amounts and suggested consideration be given as to whether more detailed information should also be released. The General Accounting Office (GAO) should be empowered to conduct audits at the request of congressional oversight committees.

Tests by intelligence agencies on human subjects of drugs or devices that could cause physical or mental harm should not occur except under stringent conditions.

The committee made a number of recommendations regarding procedures for granting security clearances and for handling classified information. It also recommended consideration of new legislative initiatives to deal with other existing problems. Finally, the Committee recommended the creation of a registry of all classified executive orders, including NSC directives, with access provided to congressional oversight committees.

Pike Committee (House Select Committee on Intelligence), 1976

The House Select Committee on Intelligence, chaired by Representative Otis G. Pike, also conducted a wide-ranging survey of intelligence activities. In the conduct of its hearings, the Pike Committee was far more adversarial to the intelligence agencies than the Senate Committee. Publication of its final report was not authorized by the House, although a version was published in a New York tabloid. The Pike Committee's recommendations, however,

were published on February 11, 1976.[81] There were some twenty recommendations, some dealing with congressional oversight, with one dealing, anomalously, with the status of the Assistant to the President for National Security Affairs.

The Pike Committee recommended that covert actions not include, except in time of war, any activities involving direct or indirect attempts to assassinate any individual. The prohibition was extended to all paramilitary operations. A National Security Council subcommittee would review all proposals for covert actions and copies of each subcommittee member's comments would be provided to congressional committees. The committee further recommended that congressional oversight committees be notified of presidential approval of covert actions within 48 hours. According to the proposal, all covert actions would have to be terminated no later than 12 months from the date of approval or reconsidered.

The committee recommended that specific legislation be enacted to establish NSA and define its role in monitoring communications of Americans and placed under civilian control.

The Pike Committee further recommended that all "intelligence related items" be included as intelligence expenditures in the President's budget and that the total sum budgeted for intelligence be disclosed.

The committee recommended that transfers of funds be prohibited between agencies or departments involved in intelligence activities. Reprogramming of funds within agencies would be dependent upon the specific approval of congressional oversight and appropriations committees. The same procedures would be required for expenditures from reserve or contingency funds.

The Pike Committee also looked at the role of the DCI. Like many others who have studied the question, it recommended that the DCI should be separate from managing any agency and should focus on coordinating and overseeing the entire intelligence effort with a view towards eliminating duplication of effort and promoting competition in analysis. It advocated that he should be a member of the National Security Council. Under this proposal the DCI would have a separate staff and would prepare national intelligence estimates and daily briefings for the President. He would receive budget proposals from agencies involved in intelligence activities. (The recommendations did not indicate the extent of his authority to approve or disapprove these recommendations.) The DCI would be charged with coordinating intelligence agencies under his jurisdiction, eliminating duplication, and evaluating performance and efficiency.

The committee recommended that the GAO conduct a full and complete management and financial audit of all intelligence agencies and that the CIA internal audit staff be given complete access to CIA financial records.

The committee recommended that a permanent foreign operations subcommittee of the NSC, composed of cabinet-rank officials, be established. This subcommittee would have jurisdiction over all authorized activities of intelligence agencies (except those solely related

---

[81] U.S. Congress, House of Representatives, 94th Congress, 2nd session, Select Committee on Intelligence, *Recommendations of the Final Report of the House Select Committee on Intelligence*, H. Rept. 94-833, February 11, 1976.

to intelligence gathering) and review all covert actions, clandestine activities, and hazardous collecting activities.

It was recommended that DIA be abolished and its functions divided between the Office of the Secretary of Defense and the CIA. The intelligence components of the military services would be prohibited from undertaking covert actions within the U.S. or clandestine activities against U.S. citizens abroad.

Relations between intelligence and law enforcement organizations were to be limited. Intelligence agencies would be barred from providing funds to religious or educational institutions or to those media with general circulation in the United States.

The committee recommended that specific legislation be considered to deal with the classification and regular declassification of information.

It was also recommended that an Inspector General for Intelligence be nominated by the President and confirmed by the Senate with authority to investigate potential misconduct of any intelligence agency or personnel. He would make annual reports to the Congress.

The committee also made recommendations regarding the organization and operations of the FBI and its role in investigating domestic groups.

In an additional recommendation, Representative Les Aspin, a member of the committee, urged that the CIA be divided into two separate agencies, one for analysis and the other for clandestine collection and covert operations. A similar recommendation was made by Representative Ron Dellums, who also served on the committee.

Clifford and Cline Proposals, 1976

In 1976 hearings by the Senate Committee on Government Operations, Clark Clifford (who had served as President Johnson's final Secretary of Defense and, in an earlier position in the Truman Administration, had been involved in legislation creating the CIA) proposed the creation of a post of Director General of Intelligence to serve as the President's chief adviser on intelligence matters and as principal point of contact with the congressional intelligence committees. There would be a separate director of the CIA whose duties would be restricted to day-to-day operations.[82]

In the same year, Ray Cline, a former Deputy Director of the CIA, made a number of recommendations[83]. He recommended that the DCI exert broad supervisory powers over the entire intelligence community and the CIA be divided into two agencies, one to undertake analytical work and the other for clandestine services. He also proposed that the DCI be given cabinet rank, a practice that would find support in both the Reagan and Clinton administrations.

---

[82]U.S. Congress, Senate, 94th Congress, 2nd session, Committee on Government Operations, *Oversight of U.S. Government Intelligence Functions*, Hearings, Jan. 21-Feb. 6, 1976, pp. 203-204.

[83]In his book *Secrets, Spies, and Scholars* (Washington: Acropolis Books, 1976).

Proposed Charter Legislation, 1978-1980

Subsequent to the establishment of permanent intelligence oversight committees in the Senate in 1976 and the House of Representatives in 1977, attention in Congress shifted to consideration of charter legislation for intelligence agencies.[84] It was envisioned that the charter legislation would include many of the recommendations made earlier by the Church and Pike Committees. Introduced by Senator Walter Huddleston and Representative Edward Boland, the draft National Intelligence Reorganization and Reform Act of 1978 (S.2525/H.R.11245, 95th Congress) would have provided statutory charters to all intelligence agencies and created a Director of National Intelligence (DNI) to serve as head of the entire Intelligence Community. Day-to-day leadership of CIA could be delegated to a deputy at presidential discretion. The draft legislation contained numerous reporting requirements (regarding covert actions in particular) to Congress and an extensive list of banned or restricted activities. The draft legislation of more that 170 pages was strongly criticized from all sides in hearings; some arguing that it would legitimize covert actions inconsistent with American ideals and others suggesting that its complex restrictions would unduly hamper the protection of vital American interests. The bills were never reported out of either intelligence committee, although the Foreign Intelligence Surveillance Act of 1978 (P.L. 95-511) provided a statutory base for electronic surveillance within the United States.

Charter legislation was also introduced in the 96th Congress. It contained many of the provisions introduced in the earlier version, but also loosened freedom of information regulations for intelligence agencies and the requirements of the Hughes-Ryan amendments of 1974 requiring that some eight committees be notified of covert actions. This legislation (S.2284, 96th Congress) came under even heavier criticism from all sides than its predecessor. It was not reported by the Senate Intelligence Committee, but other stand-alone legislation did pass and a shorter bill reducing the number of committees receiving notification of covert actions--and "significant anticipated intelligence activities"--was introduced and eventually became law in October 1980 as part of the FY1981 Intelligence Authorization Act (P.L. 96-450).

The Executive Branch Response, 1976-1981

Concurrent with, and subsequent to, these legislative initiatives, the Executive Branch, in part to head off further Congressional action, implemented some of the more limited recommendations contained in their respective proposals. Presidents Gerald Ford, Jimmy Carter, and Ronald Reagan each issued detailed Executive Orders (E.O.) setting guidelines for the organization and management of the U.S. Intelligence Community.

Issued by President Ford on February 18, 1976, prior to the release of the Church and Pike Committee findings, Executive Order 11905 undertook to implement some of the more limited recommendations of the Rockefeller and Murphy Commissions. In particular, E.O. 11905 identified the DCI as the President's primary intelligence advisor and the principal spokesman for the Intelligence Community and gave him responsibilities for developing the

---

[84]The effort to pass intelligence charter legislation is described in John M. Oseth, *Regulating U.S. Intelligence Operations: A Study in Definition of the National Interest* (Lexington, KY: University Press of Kentucky, 1985); also, Frank J. Smist, Jr., *Congress Oversees the United States Intelligence Community, Second Edition, 1947-1994* (Knoxville, TN: University of Tennessee Press, 1994).

National Foreign Intelligence Program (NFIP). It also delineated responsibilities of each intelligence agency, provided two NSC-level committees for internal review of intelligence operations, and established a separate three-member Intelligence Oversight Board to review the legality and propriety of intelligence activities. It placed restrictions on the physical and electronic surveillance of American citizens by intelligence agencies.[85]

On January 24, 1978, President Carter issued Executive Order 12036, that superseded E.O. 11905.[86] Carter's Executive Order sought to define more clearly the DCI's community-wide authority in areas relating to the "budget, tasking, intelligence review, coordination and dissemination, and foreign liaison."[87] In particular, it formally recognized the establishment of the National Foreign Intelligence Program budget and the short-lived National Intelligence Tasking Center (NTIC), that was supposed to assist the DCI in "translating intelligence requirements and priorities into collection objectives."[88] E.O. 11905 also restricted medical experimentation and prohibited political assassinations.

President Reagan continued the trend towards enhancing the DCI's community-wide budgetary, tasking, and managerial authority. On December 4, 1981, he issued Executive Order 12333, detailing the roles, responsibilities, missions, and activities of the Intelligence Community. It supplanted the previous orders issued by Presidents Ford and Carter. Fifteen years later, E.O. 12333 remains the governing executive branch mandate concerning the managerial structure of the Intelligence Community.

E.O. 12333 designates the DCI "as the primary intelligence advisor to the President and NSC on national foreign intelligence."[89] In this capacity, the DCI's duties include the implementation of special activities (covert actions), liaison to the nation's foreign intelligence and counterintelligence components, and the overall protection of the community's sources, methods, and analytical procedures.[90] It grants the DCI "full responsibility for [the] production and dissemination of national foreign intelligence," including the authority to task non-CIA intelligence agencies, and the ability to decide on community tasking conflicts.[91] The order also sought to grant the DCI more explicit authority over the development, implementation, and evaluation of NFIP.[92]

---

[85]Executive Order 11905, February 18, 1976, United States Foreign Intelligence Activities, as summarized in Alfred B. Prados, *Intelligence Reform: Recent History and Proposals*, CRS Report 88-562 F, August 18, 1988, p. 18; hereafter cited as Prados, 88-562 F.

[86]Executive Order 12036, January 24, 1978, United States Intelligence Activities; hereafter cited as Executive Order 12036.

[87]Lowenthal, p. 107.

[88]Bruce W. Watson, Susan M. Watson, and Gerald W. Hopple, *United States Intelligence: An Encyclopedia* (New York: Garland Publishing, 1990), p. 231.

[89]Section 1.5(a), Executive Order 12333, December 4, 1981, *United States Intelligence Activities.*

[90]Executive Order 12333, Section 1.5 (d,e,h).

[91]Executive Order 12333, Section 1.5(k,h).

[92]Lowenthal, p. 107.

To a certain extent, E.O. 12333 represented a relaxation of the restrictions placed upon the community by Carter. Although it maintained the prohibition on assassination, the focus was on "authorizations" rather than "restrictions." "Propriety" was removed as a criterion for approving operations. Arguably, the Reagan Administration established a presumption in favor of government needs over individual rights.[93] However, in the absence of legislation, the DCI continued to lack statutory authority over all aspects of the Intelligence Community, including budgetary issues.

The Turner Proposal, 1985

In 1985, Admiral Stansfield Turner, DCI in the Carter Administration, expressed his views on the need for intelligence reform[94]. In part, Turner recommended reducing the emphasis on covert action and implementing a charter for the Intelligence Community. The most important recommendation involved the future of the DCI of which Turner maintained:

The two jobs, head of the CIA and head of the Intelligence Community, conflict. One person cannot do justice to both and fulfill the DCI's responsibilities to the President, the Congress, and the public as well.[95]

Turner went on to propose the separation of the two jobs of DCI and head of the CIA with the creation of a Director of National Intelligence, separate and superior to the CIA. Turner also recommended placing less emphasis on the use of covert action than the Reagan Administration.

Iran-Contra Investigation, 1987

During highly publicized investigations of the Reagan Administration's covert support to Iran and the Nicaraguan Resistance, the role of the Intelligence Community, the CIA, and DCI Casey were foci of attention. Much of the involvement of National Security Council staff was undertaken precisely because legislation had been enacted severely limiting the role of intelligence agencies in Central America and because efforts to free the hostages through cooperation with Iranian officials had been strongly opposed by CIA officials. The executive branch's review, chaired by former Senator John Tower, expressed concern that precise procedures be established for restricted consideration of covert actions and that NSC policy officials had been too closely involved in the preparation of intelligence estimates.[96] The

---

[93]See Oseth, *Regulating U.S. Intelligence Operations*, especially p. 155.

[94]In his book *Secrecy and Democracy: The CIA in Transition* (Boston: Houghton Mifflin, 1985).

[95]*Secrecy and Democracy*, p. 273.

[96]U.S., President's Special Review Board, *Report*, 1987, pp. V-5--V-6.

investigation of the affair by two congressional select committees resulted in a number of recommendations for changes in laws and regulations governing intelligence activities.

Specifically the majority report of the two congressional select committees that investigated the affair made a number of recommendations regarding presidential findings concerning the need to initiative covert actions. Findings should be made prior to the initiation of a covert action, they should be in writing, and they should be made known to appropriate Members of Congress in no event later than forty-eight hours after approval. Further, the majority of the committees urged that findings be far more specific than some had been in the Reagan Administration. Statutory inspector general and general counsels, confirmed by the Senate, for the CIA were also recommended.[97] Minority members of the two committees made several recommendations regarding congressional oversight, urging that on extremely sensitive matters that notifications of covert actions be made to only four Members of Congress instead of the existing requirement for eight to be notified.[98]

These recommendations were subsequently considered by the two intelligence committees. A number of provisions was enacted dealing with covert action findings in the Intelligence Authorization Act for FY1991 (P.L. 102-88).

Boren-McCurdy, 1992

A major legislative initiative, reflecting the changed situation of the post-Cold War world, began in February 1992, when Senator David Boren, the Chairman of the Senate Select Committee on Intelligence, and Representative Dave McCurdy, the Chairman of the House Permanent Select Committee on Intelligence, announced separate plans for an omnibus restructuring of the U.S. Intelligence Community, to serve as an intelligence counterpart to the Goldwater-Nichols Department of Defense Reorganization Act of 1986. The two versions of the initiative (S. 2198 and H.R. 4165, 102nd Congress) differed in several respects, but the overall thrust of the two bills was similar. Both proposals called for:

- Creating a Director of National Intelligence (DNI) with authority to program and reprogram intelligence funds throughout the Intelligence Community, including the Defense Department, and to direct their expenditure; and to task intelligence agencies and transfer personnel temporarily from one agency to another to support new requirements;

- Creating two Deputy Directors of National Intelligence (DDNIs); one of whom would be responsible for analysis and estimates, the other for Intelligence Community affairs;

---

[97]U.S. Congress, 100th Congress, 1st session, Senate Select Committee on Secret Military Assistance to Iran and the Nicaraguan Opposition and U.S. House of Representatives Select Committee to Investigate Covert Arms Transactions with Iran, *Report of the Congressional Committees Investigating the Iran-Contra Affair with Supplemental, Minority, and Additional Views*, S.Rept. 100-216/H. Rept. 100-433, November 17, 1987, pp. 423-427; hereafter cited as the Iran-Contra Report.

[98]Iran-Contra Report, pp. 583-586.

- Creating a separate Director of the CIA, subordinate to the new DNI, to manage the agency's collection and covert action capabilities on a day-to-day basis;

- Consolidating analytical and estimative efforts of the Intelligence Community (including analysts from CIA, and some from DIA, the Bureau of Intelligence and Research (INR) at the State Department, and other agencies) into a separate office under one of the Deputy DNIs (this aspect of the proposal would effectively separate CIA's analytical elements from its collection and covert action offices);

- Creating a National Imagery Agency within the Department of Defense (DOD) to collect, exploit, and analyze imagery (these tasks had been spread among several entities; the House version would divide these efforts into two new separate agencies).

- Authorizing the Director of DIA to task defense intelligence agencies (DIA, NSA, the new Imagery Agency) with collection requirements; and to shift functions, funding, and personnel from one DOD intelligence agency to another;

This major restructuring effort would have provided statutory mandates for agencies where operational authority was created by executive branch directives. Both statutes and executive branch directives provided the DCI authority to task intelligence agencies outside the CIA and to approve budgets and reprogramming efforts; in practice, however, this authority had never been fully exercised. This legislation would have provided a statutory basis for the DCI (or DNI) to direct collection and analytical efforts throughout the Intelligence Community.

The Boren-McCurdy legislation was not adopted, although provisions were added to the FY1994 Intelligence Authorization Act (P.L. 102-496) that provided basic charters for intelligence agencies and set forth in law the DCI's coordinative responsibilities *vis-à-vis* intelligence agencies other than the CIA. Observers credited strong opposition from the Defense Department and concerns of the Armed Services Committees with inhibiting passage of the original legislation.

Commission on the Roles and Capabilities of the U.S. Intelligence Community (Aspin Commission), 1995-1996

Established pursuant to the Intelligence Authorization Act for FY 1995 (P.L. 103-359) of September 27, 1994, the Commission on the Roles and Capabilities of the U.S. Intelligence Community was formed to assess the future direction, priorities, and structure of the Intelligence Community in the post-Cold War environment. Originally under the chairmanship of the late Les Aspin, the commission was subsequently headed by former Secretary of Defense Harold Brown. Nine members were appointed by the president and eight nominated by the congressional leadership. A final report was scheduled for March 1996.

P.L. 103-359 set forth nineteen separate issues for the commission to address, including a determination of intelligence needs and priorities in the post-Cold War world, whether or not existing organizational arrangements provide the most effective and efficient framework to meet those needs, and what resources will be necessary to satisfy these requirements.

Specifically, the commission was asked to examine such issues as the need to maintain the CIA as a separate entity, U.S. counterintelligence efforts, and the managerial structure of intelligence components in the armed services. In an era of budgetary constraints and evolving policy concerns, the commission also was expected to address personnel issues, allocations of resources, duplication of services, expanded use of open source intelligence, and the viability of maintaining a covert action capability. The future responsibilities and authorities of the DCI were indicated to be a paramount concern.

PART II

Advantages and Disadvantages of Major Proposals

Many of the recommendations contained in commission reports and legislative initiatives have been--at least in part--adopted either by Executive Order, through other executive branch initiatives, or in statutory law. A number of the issues raised by commissions and with other proposals have been addressed in the context of annual authorization bills (and occasionally through appropriations laws). Many observers believe that this process has proven effective since issues can be dealt with on a case-by-case basis as they appear most urgent. Charter legislation, on the other hand, inevitably involves broad questions relating not only to intelligence, but to defense and foreign policy. The legislative effort involved in sorting out the complexities of such concerns and holding together a coalition for many months is perceived as more difficult than including less ambitious provisions in annual authorization bills. The annual authorization process is not, however, necessarily smooth; in November 1990, President Bush pocket-vetoed an intelligence authorization bill and a replacement was not signed until the following August; the FY1996 Intelligence Authorization Act was not signed until more than three months into the new fiscal year.

Although a consolidated legislative charter has not been enacted for the Intelligence Community, legislation has addressed the preponderance of issues that have been raised by commissions and investigatory committees. Title VII of the Intelligence Authorization Act for FY1993 (P.L. 102-496) included provisions defining the role of the DCI and the responsibilities of the Secretary of Defense pertaining to national intelligence activities. In so doing, it provided a statutory basis for intelligence agencies beyond that which they had been granted in previous legislation. Earlier statutes relating to some intelligence agencies primarily concerned buildings and personnel rather than operational missions.

A series of laws has also been enacted governing procedures for implementing covert actions.[99] There has been extended controversy on the extent of notice that presidents should provide to Congress concerning such actions; presidents continue to assert a constitutional right to initiate covert actions without notifying Congress in extreme circumstances. Although many in Congress remain opposed to this assertion, observers consider that, on the whole, current procedures are adequate, as long as reasonably good will prevails between the executive and legislative branches.

CIA Inspectors General are now nominated by the President and confirmed by the Senate; legislation to require presidential appointment of the CIA General Counsel was rejected in

---

[99]Reporting of covert actions was most recently addressed in Title VI of the Intelligence Authorization Act for FY1991 (P.L. 102-88) which incorporated changes that reflected judgments of previous weaknesses revealed in the Iran-Contra Affair. Some in Congress had intended to include a provision requiring that Congress be provided prior notice of covert actions (or, in emergencies, within 48 hours of initiation), but the Bush Administration expressed strong opposition and asserted a Constitutional right for the President to undertake covert actions when necessary. The Conference Committee that met on the FY1991 bill noted that neither intelligence committee had ever accepted that the Constitution allowed the President to exercise such authority, but added: "The conferees recognize that this is a question that neither they nor the Congress itself can resolve. Congress cannot diminish by statute powers that are granted by the Constitution. Nor can either the legislative or executive branch authoritatively interpret the Constitution, which is the exclusive province of the judicial branch." U.S. Congress, House of Representatives, 103rd Congress, 1st session, Committee of Conference, *Intelligence Authorization Act, Fiscal Year 1991*, H. Rept. 102-166, July 25, 1991, p. 28.

the 103d Congress.[100] Little, if any, consideration has been given to limiting the term of the DCI to 10 years, since all recent DCIs have had much shorter tenures. There exists considerable feeling that presidents must have a degree of confidence in their DCIs that could not exist in a person who does not serve at the president's pleasure.

Another area of concern reflected in many recommendations is the potential for intelligence agencies to infringe on the rights of U.S. citizens. Such concerns fueled the Church and Pike investigations as well as others. Congress has addressed these issues in several pieces of legislation, including the Foreign Intelligence Surveillance Act of 1978 and the Classified Information Procedures Act of 1980 (P.L. 96-456). Legislation relating to warrantless wiretaps and physical searches was enacted as part of the Intelligence Authorization Act for FY1995 (P.L. 103-359). Questions regarding the proper coordination of intelligence collection by the CIA and the FBI were, however, raised anew in the aftermath of the Oklahoma City bombing.

A Counterintelligence Policy Board was established, and closer cooperation between the CIA and the FBI on counterintelligence issues mandated, in Section 811 of the FY1995 Intelligence Authorization Act (with the FBI granted a more important role). The FY1996 Intelligence Authorization Act (P.L. 104-93) provided the FBI with enhanced authority to acquire information for counterintelligence purposes.

Congress and the executive branch have addressed most of the issues raised by commissions and individual legislators; the results inevitably have not been universally popular. Some continue to seek broader restrictions, if not outright prohibitions of covert actions. Drafting regulations and statutes on classification continues to be contentious. As is the case with any group of federal agencies, there is likely to be a continuing need to adapt the regulations and statutes dealing with the Intelligence Community to changing conditions and public opinion.

There remain, nonetheless, several areas of continuing concern that have been addressed by commissions and Members over the years that some believe have never been adequately resolved by Congress or the executive branch. The extent of the DCI's authority over agencies other than the CIA, the role and control of covert actions, and the question of making public the total amount of intelligence spending are of continuing interest. These remain controversial among informed observers and all may be revisited during the 104th Congress (along with the somewhat more narrow question of requiring confirmation of the CIA's General Counsel). The positions of those who support and oppose various proposals are indicated where possible, but in many cases the views noted may only reflect those held at one point in time.

Role of the DCI

Almost all reform and reorganization proposals through the years have addressed, directly or indirectly, the role of the DCI, and his relationship to the CIA and with other intelligence agencies. Statutory authorities dating from the National Security Act of 1947 give the DCI direct operational control of the CIA. He has, in addition, acquired by statute and presidential

---

[100]The original Senate version of the intelligence authorization act for FY1995 (S. 2082, 103d Congress) contained provisions requiring Presidential nomination and Senate confirmation of CIA's general counsel, but support from House conferees was not forthcoming.

direction a degree of influence over the budgetary and operational practices of other intelligence agencies. Most DCIs, however, have chosen (or have been directed) to concentrate their energies on the CIA. Stansfield Turner, DCI under President Carter, was perhaps the DCI most inclined to focus on community-wide concerns. The current DCI, John M. Deutch, following his Pentagon experience, is making vigorous efforts to integrate intelligence activities of different agencies. On the other hand, some DCIs, including those who were most concerned with clandestine operations, such as Allen Dulles, Richard Helms, William Colby, and William Casey, tended not to concentrate on community-wide programs. The personal inclinations of DCIs and Presidents will, it seems, inevitably influence the relative emphasis that is given to community-wide issues.

As noted above, some commissions and legislators, perceiving a need for more centralized direction and coordination of the Intelligence Community, have proposed that the DCI be given more authority over all intelligence agencies, specifically in terms of approving budgets, directing collection and analytical tasks, realigning functions, and transferring personnel among agencies. Some have suggested that the senior intelligence official be given the title of Director of National Intelligence (DNI) with a separate position created for the head of the CIA who would have responsibility for the day-to-day management of the agency.

Arguments In Favor. Intelligence activities and spending are spread over many agencies and offices, some of which duplicate the work of others; given the end of the Cold War and tight budgetary constraints throughout the federal government, one individual is needed to coordinate and rationalize the nation's intelligence effort, eliminating waste and duplication of effort. Heretofore, despite having been given some authority to review other agency budgets, DCIs have lacked meaningful authority to change budgets, initiate or eliminate programs, and move personnel from one agency to another. The large intelligence agencies of the Defense Department that account for the bulk of intelligence spending, in particular, have been more responsive to the practical needs of senior military officers and the OSD staff than to the DCI. Many of DCI Turner's efforts to merge national and tactical intelligence activities in the late 1970s were, however, successfully resisted by DOD. Despite subsequent efforts to enhance the authority of the DCI, DOD retains enormous influence over both national and tactical systems.

Existing arrangements, according to this view, have resulted in faulty coordination, waste, duplication of effort, and a failure to provide the best available intelligence support to customers. Agencies, especially the DOD intelligence agencies, have set their own agendas, procured their own equipment, and developed their own programs with insufficient attention to efforts underway elsewhere. In some cases, expensive technologies and/or scarce human agents have been directed to acquire data that could have been obtained from open sources. A major problem area has been a failure by the leadership of the Intelligence Community to prioritize collection requirements adequately. Too often collection efforts have been undertaken more because the technology and administrative infrastructure existed rather than as a result of significant operational or policy needs.

Despite having certain responsibilities for the entire Intelligence Community, DCIs for the most part have concentrated on the management of the CIA (and especially the Operations Directorate). Efforts to coordinate the activities of all agencies have been distinctly secondary. To remedy the problem indicated, fundamental statutory changes are required. The DCI would have to be given "line" authority over all intelligence organization, or at least the larger ones--NSA, CIA, NRO, and DIA. Budget authority would have to be appropriated to him and he

would have to be given authority to move personnel from agency to agency as needed and to consolidate and direct the activities of the entire community. The creation of the Intelligence Community Staff in 1972 ultimately proved inadequate as it became immersed in technical budgetary staffwork and failed to exert significant leadership of the community. It was replaced in 1992 by the Community Management Staff (CMS) with similar functions but working more closely for the DCI. There is some question that the CMS can resolve the perceived difficulties without changes in the DCI's statutory authorities.

Adherents of this view usually indicate that the DCI (or DNI) should not involve himself directly in the day-to-day management of the CIA, but concentrate on community-wide issues. They see him as functioning at the White House level in a manner similar to the OMB Director. These arguments have been put forth, in varying forms, by many observers including Schlesinger, Clifford, Cline, the Pike Committee, and in the Boren/McCurdy bills.

Arguments in Opposition. Those who have opposed the above line of argument believe that any separation of the DCI from the management of the CIA would render him far less influential. To a considerable extent, influence in policy derives from institutional functions and, if the DCI had only a small personal staff, he would become merely another White House aide. Power would gravitate to the person who was actually directing the extensive daily affairs of the CIA.

The major DOD intelligence agencies are closely related to military combat functions and are staffed with active-duty military personnel. The needs of military commander differ from those of policymakers. Placing them under a civilian official not in the military chain of command would undercut the vital principle of unity of command; it could result in the subordination of the needs of combat forces to civilian concerns and a genuine decrease in military capabilities. The approach might also encourage a tendency within DOD to establish rudimentary and less capable intelligence entities under the direct control of military commanders. Strong opposition to this approach has been set forth by Secretaries of Defense (especially by Secretary Richard Cheney in comments on the Boren-McCurdy proposals). Admiral Bobby Inman, who had served as Director of NSA and Deputy DCI, has noted that "I suspect if you query the former Directors of Central Intelligence, none will support [separating the leadership of the Community from management of CIA], because they all remember the support they got primarily from CIA for carrying out their missions. And they worry that without that they would not be effective in this city. I have even heard the phrase used, that they would be like the Drug Czar.[101]

Some opponents of increasing the statutory authority of the DCI do not believe that current procedures for coordinating intelligence collection and analysis are inappropriate. In many cases, they argue, those closest to collection systems have the best insight into ways to optimize collection. Moreover, analysts in various agencies know which problems are of greatest concern to senior officials. The creation of a separate DNI would add another layer of staff not closely connected to ongoing needs for intelligence support to policymakers and military commanders.

Others acknowledge that real problems exist with coordination and duplication of effort, but believe that current authorities are adequate. The problems stem from inattention by

---

[101] Testimony reprinted in U.S. Congress, Senate, 102nd Congress, 1st session, Select Committee on Intelligence, *Review of Intelligence Organization*, Hearing, S. Hrg. 102-91, March 21, 1991, p. 23.

previous DCIs and, perhaps, poor appointments to leadership positions in the Intelligence Community. They believe that a rigorous exploitation of existing authorities and creative use of the Community Management Staff could allow the DCI to coordinate intelligence activities far more effectively than has been done previously. The earlier efforts by DCI Turner were in part misconceived and, in any event, affected by Cold War issues that are no longer relevant. Now, it is argued, a new approach can be taken to bring intelligence agencies into closer alignment.

Role of the CIA Operations Directorate

A number of proposals have been made over the years to separate analytical functions from the covert operations that in the popular media constitute the main function of intelligence agencies (although in recent years they absorb only a small percentage of the intelligence budget). Clandestine activities include both human intelligence (HUMINT) collection as well as covert actions; there is considerable use of the same personnel for both duties.

Arguments in Favor. Covert actions are, to some critics, antithetical to democratic values and have often undermined American interests and the country's reputation. The continued existence of a sizable CIA Directorate of Operations provides policymakers with a readily available instrument to pursue policies that would not stand up to public scrutiny, especially in the post-Cold War world. Furthermore, there is in CIA's Operations Directorate a culture of secrecy and deceit that some contend has come to permeate the entire agency.

If, under exceptional circumstances, the national interest requires that covert actions be undertaken, a small office separated from the CIA, perhaps under DOD control, would be more appropriate. Separating or abolishing it would improve the image of the U.S. government throughout the world and would reflect a renewed American commitment to human rights and democracy. Separation would further help ensure that CIA analysis is not skewed to support or justify the work of the Operations Directorate.

Some observers also argue that intelligence analysts should be in close touch with academic scholars, journalists, and others with insight into foreign developments. Especially in an era of diverse threats and opportunities, the Intelligence Community must have access to contacts and analytical resources available in the civilian sector, as it cannot maintain the depth of expertise on each area of the world that it once maintained on the Soviet Union, the Warsaw Pact, and China. In Third World areas, the best available information may come from area specialists in universities and from journalists with long experience in the region. The role of the CIA in undertaking covert actions, and the sustained attention these efforts receive in the media, complicate the CIA's relationships with academic and other civilian scholars. The well-known hostility to the CIA among many scholars usually derives from opposition to covert actions (and to the policies that incorporate them) rather than to the agency's analytical products.

Few, other than those who would abolish the CIA, argue against the need for the centralized gathering and analysis of information. Although intelligence professionals tend to consider the transfer of hostility to covert actions to encompass all intelligence activities ill-founded and unfair, it is a fact of life that effects the Intelligence Community's ability to provide the best available intelligence to policymakers. The CIA would be best served if covert actions could be undertaken by a smaller separate organization, perhaps one positioned outside the Intelligence Community. While there would probably be some duplication of effort between a separate covert action organization and CIA clandestine collection efforts, the merits

of improving the CIA's analytical reputation would outweigh any overlap. Such arguments have been made by Ray Cline, former Representative Aspin, and, earlier, by Professor Harry Howe Ransom.[102] They were also reflected in the Boren-McCurdy proposals.

Arguments in Opposition. Those who support the retention of the Operations Directorate within the current CIA organization argue that any separate covert action organization would complicate the nation's intelligence efforts by creating still another agency with its own institutional interests, thereby making centralized coordination more difficult. There have been instances of covert operatives working at cross purposes in the field, and inevitable compartmentalization will complicate efforts of senior policymakers to gain an understanding of information held in all parts of the U.S. government about a given foreign situation.

These observers further argue that there is no valid need to protect analysts from the "grimy real world the collectors deal with." Intelligence analysts, they argue, are not academic specialists but government officials responsible for providing warning of threats to the national security. They need, accordingly, the closest contact with those engaged in intelligence collection and operations. Such views have been set forth by former DCI Colby and former senior CIA official George Carver.[103]

A Third View. Still other observers have argued that covert actions have never been specifically authorized by statute and that the CIA's conduct of them is legally questionable (although provisions for the reporting of presidential authorizations have been enacted).[104] Those holding this view would probably oppose an agency specifically established to undertake covert actions and further argue that covert actions are contrary to the national interest and the U.S. should set an example by forswearing them.

Disclosing the Intelligence Budget

Many observers of the Intelligence Community have long recommended that the overall intelligence budgets be publicly disclosed.[105] Since the creation of the CIA, intelligence spending for the larger intelligence agencies has largely been "hidden" in DOD authorization and appropriations legislation whose totals also include other classified accounts. This has not been the case for the State Department's Bureau of Intelligence and Research, the CIA Retirement and Disability Fund, and some other functions. The actual figures are available to Members of Congress and to executive branch officials with a need-to-know, but are not

---

[102]See Ransom's *The Intelligence Establishment* (Cambridge, Mass: Harvard University Press, 1970), pp. 246-247.

[103]U.S. Congress, House of Representatives, 102d Congress, 2d session, Permanent Select Committee on Intelligence, *H.R. 4165, National Security Act of 1992*, Hearings, Part I, March 4, and 11, 1992, especially pp. 38-39, 191-192.

[104]See the comments contained in a February 20, 1992 letter from the American Civil Liberties Union, reprinted in U.S. Congress, 102d Congress, 2nd session, Select Committee on Intelligence, U.S. Senate, and Permanent Select Committee on Intelligence, House of Representatives, *S. 2198 and S. 421 to Reorganize the United States Intelligence Community*, Joint Hearing, S. Hrg 102-1052, April 1, 1992, pp. 96-97.

[105]For additional background, see Richard A. Best, Jr. and Elizabeth B. Bazan, *Intelligence Spending: Should Total Amounts Be Made Public?*, CRS Report 94-261F, March 22, 1994.

made public. In recent years, there has been widespread media discussions of a given multi-billion dollar figure and the House Appropriations Committee in 1994 released testimony that described dollar amounts included in the Administration intelligence spending request for FY1995.[106] Congress has twice gone on record (in the FY1992 and FY1993 intelligence authorization acts) *urging* that "the aggregate amount requested and authorized for, and spent on, intelligence and intelligence-related activities should be disclosed to the public in an appropriate manner." In 1993, 1994, and 1995, however, Congress rejected floor amendments to release intelligence budget totals.

Arguments in Favor. The principal argument by those in favor of making intelligence spending levels public is based on constitutional provisions requiring regular statements and accounts of public spending (Article I, Section 9, Clause 7). Even if obscuring intelligence spending is considered technically legal, given the end of the Cold War it is unwise and unnecessary. The public has a right to know how taxmonies are being spent. The Church and Pike Committees made this point, as have numerous other observers in more recent years.

The secrecy that surrounded the Cold War superpower competition is no longer needed. Even if potential enemies learn how much the United States is spending on intelligence, the information will not assist them. There are unlikely to be any bulges in intelligence spending that would alert them to new American capabilities, and current surveillance systems are widely known. Similarly, it is unlikely that additional U.S. resources directed at a new target would be of sufficient size to create a noticeable increase in total intelligence spending and alert the targeted country. Public discourse regarding intelligence priorities will be enhanced and intelligence activities ultimately improved through the democratic process. Some former senior intelligence officials have come to support public disclosure of total expenditures, including former DCI Turner and Admiral Inman. The current DCI, John Deutch, has stated that disclosing the aggregate total figure for intelligence spending would cause no harm to national security.

Arguments in Opposition. Intelligence spending has been kept secret since the early days of the Republic in order to avoid making potentially hostile foreign powers even generally aware of American efforts. Although the international situation has changed dramatically in recent years, publicity surrounding intelligence spending inevitably complicates the conduct of the nation's foreign policy and gives potential adversaries a propaganda boon as well as official notice of U.S. activities and capabilities. Secrecy, they argue, is the prerequisite for intelligence collection and evaluation and spending levels can be a prime indicator of U.S. programs. Such arguments were made by former DCI James Woolsey for the Clinton Administration and by Robert Gates when he served as DCI in the Bush Administration (although at one earlier point he had indicated flexibility on the issue).

There are two arguments often made by those opposed to making total figures for intelligence spending public; they are described colloquially as the "slippery slope" and the "rabbit in the snake." The former refers to the difficulty of making public a single figure for intelligence spending without immediately having to set forth an elaborate explanation of what is included and what is excluded. The resulting discussion and cost breakouts would

---

[106]U.S. Congress, House of Representatives, 103rd Congress, 2nd session, Committee on Appropriations, Subcommittee on the Department of Defense, *Department of Defense Appropriations for 1995*, Hearings, Part 3, 1994, pp. 717, 784.

eventually and inevitably result in revealing virtually every aspect of intelligence spending and reveal legitimate areas of secrecy. The "rabbit in the snake" argument suggests that large changes in intelligence spending in a single year would reveal to foreign governments or hostile groups the introduction of new collection systems and allow them to take countermeasures. It is recalled that the advent of satellite systems had produced just such an increase, and information concerning the pace and extent of the U.S. effort would have been highly valuable to Soviet leaders had they had access to budgetary totals.

Some opposed to releasing budgetary data also suggest that publishing numbers without extensive explanation could easily mislead the public. Some tactical intelligence programs, for instance, could be moved out of the intelligence budget to justify claims of a major decline in intelligence spending when in fact there had been no net savings to the taxpayers. Maneuvering some tactical programs into non-intelligence accounts in order to present a lower overall intelligence budget figure would further, some would argue, undermine the influence of the DCI (and, potentially, congressional intelligence oversight committees) and hamper efforts to closely coordinate expensive national and tactical programs.

Conclusion

The efforts of commissions and individuals to encourage restructuring of the U.S. Intelligence Community have led to numerous changes through internal agency direction, presidential directives, and new statutes. The general trend has been towards more thorough oversight both by the executive branch and by congressional committees. The position of the DCI has been considerably strengthened and DCIs have been given greater staff and authority to exert influence on all parts of the Community. They have not, however, been given "line" authority over agencies other than the CIA and the influence of the Defense Department remains pervasive (and, in view of the Clinton Administration's emphasis on intelligence support to military operations, may actually increase). It is unquestionable that oversight is now more thorough and that some questionable practices have ended. Congress and the incumbent president now share a degree of responsibility for covert actions.

Judgments on the efficacy of legislative and executive branch responses to recommendations made by commissions and outside experts lie beyond the scope of this paper. Some observers believe that issues raised by the commissions and individuals noted above have largely been dealt with, for better or worse. They suggest that the new issues that have arisen in the aftermath of the Cold War and as a result of technological innovations require new and different organizational responses. The advent of highly sophisticated surveillance and communications technologies, the blurring of distinctions between foreign and domestic challenges represented by terrorists and narcotics traffickers, the spread of U.S. security concerns to long-obscure regions of the world should be competently dealt with and, in any event, are grist for new commissions and new recommendations.