XV. DEPARTMENT OF DEFENSE

The Department of Defense is the nation's primary consumer of intelligence information. It controls nearly 90 percent of the nation's spending on intelligence programs, and most technical collection systems are developed, targeted, and operated by DOD personnel. The sheer size and complexity of the Defense intelligence establishment make it difficult to comprehend the problems and issues which confront policymakers and intelligence managers. Overall security needs and bureaucratic interests, as well as differing intelligence needs, further complicate the quest for solutions to the community's substantive problems and impede efforts aimed at implementing management reform.

This section of the report summarizes the Committee's investigation into the intelligence activities of the Department of Defense. It is limited in content to information that can be released publicly. Although many significant factual details about the national intelligence apparatus are thus not included, the Committee does not believe that such omissions seriously detract from a clear presentation of the central findings of its work.

The Committee focused on national intelligence activities, i.e., those which produce information primarily of interest to national decisionmakers. Tactical intelligence activities, which are organic to or in direct support of operational units, received less attention. This area could not be ignored, however, because new collection and processing technology has significantly affected the relationship between the national intelligence systems and the operational commands.

After an initial review of the entire defense intelligence program, based on documents, briefings, and studies provided by the executive branch, the Committee investigated the following issues of particular interest:

—The resource management and organizational dimensions of the Defense national intelligence community.
—The role of the Defense Intelligence Agency in relation to the CIA and intelligence functions of the military departments.
—The monitoring and reporting activities of the National Security Agency.
—Military counterintelligence and investigative activities of the Department of Defense.
—The chemical and biological research of the Department of Defense as it relates to intelligence missions.

The investigation revealed abuses of authority in all these subject areas, some of which were already known to the intelligence community, Congress, or the public. After a brief review of the relation

of intelligence to the major objectives of U.S. military forces, and the history and evolution of intelligence organizations, this report addresses these specific Defense intelligence issues in turn. The concluding section assesses the future requirements for Defense intelligence, particularly as they are affected by technological developments.

A. Objectives and Organization of the Defense Intelligence Community

The mission of the Department of Defense intelligence apparatus is to provide the defense establishment with accurate and timely information on the military capabilities or political intents of foreign states to assure that U.S. policymakers are forewarned of, and U.S. military forces prepared for, any event which threatens the national security.

There are several important consumers of Defense intelligence. National security policymakers are interested in three areas of national importance: crisis management, which calls for not only advance warning of possible military, economic, or political disruption, but also continued, detailed tracing of developments once they are underway; long-range trends in foreign military, economic, and scientific capabilities, and political attitudes which might warrant a major U.S. response; and the monitoring or verification of specific international agreements which are either in force, such as the SALT agreement or the Middle East ceasefire, or contemplated, such as Mutual and Balanced Force Reductions talks in Europe.

Defense planners, responsible for designing the structure of U.S. military forces, constitute a second important group of intelligence consumers. Although their interests are less far-ranging than those of the policymakers, their demands for insights into the capabilities of opposing military forces are generally phrased in broader terms than other DOD intelligence consumers, if only because the macroscopic analysis which supports major force structure decisions is seldom sensitive to detailed intelligence inputs.

In contrast to the estimative character of the intelligence products most required by policymakers and defense planners, two other consumer groups, the developers of weapon systems and the operating field forces, have greater interest in detailed, factual information. Satisfaction of these demands is generally more a matter of collection and compilation than analysis and inference. The major distinction between the two groups lies in their subject interests. The weapon systems developers emphasize scientific and technical detail regarding the operating characteristics and performance parameters of foreign weapon systems (knowledge of which can be useful in optimizing the design of U.S. systems). The military field commands emphasize "order of battle" data, or the unit identities and the strength, equipage, and disposition of opposing field forces.

The sequence of operations in meeting the intelligence demands of these disparate groups of consumers involves three (or, in the case of signals intelligence, four) basic steps: (1) collection—the gathering of potentially relevant data; (2) production—the translation of

these data into finished intelligence products through screening, analysis, and drawing of inferences; and (3) dissemination—delivery of the finished products to the right consumers at the right time. If the collected data are in the form of electronic signals, another step, "processing," between the first and the second, is required to refine the raw signals before they are submitted for human evaluation during the production phase.

A brief review of the major objectives of U.S. military forces may help to place the intelligence contribution in perspective.

1. Objectives of U.S. Military Forces

The paramount objective of U.S. forces is to deter nuclear attacks upon the United States and its allies by maintaining an unambiguous capability to inflict massive damage on the attacker, even after absorbing a first strike by the aggressor's nuclear forces. The defense intelligence community supports this objective by monitoring the technical developments and force deployments of potential enemies, especially those which might attempt to gain the capability for a disarming first strike. U.S. technical collection systems are able to alert leaders to an imminent attack by detecting movement or changes in the status of the Soviet Union's strategic forces. Thus warned, the United States can counter and react to such changes. This so-called strategic warning may be essential to the survival of some components of the U.S. retaliatory force.

Tactical warning, based on indications that a nuclear attack has actually commenced, is the primary responsibility of the alert and warning networks of the operational military commands. Although U.S. intelligence collection systems are not designed specifically to provide such warning, they have some inherent ability to do so. It is generally agreed that no measures would prevent a nuclear exchange from devastating all the participants; thus, relatively little attention has been devoted to developing intelligence systems designed to improve the outcome of an all-out nuclear war for the United States or its allies.

The second purpose of U.S. forces is to deter conventional (i.e., nonnuclear) military attacks on its allies. Although U.S. nuclear forces, both strategic and theater, contribute to this objective by introducing the threat of escalation into a potential aggressor's calculation, the general purpose forces (land combat, naval, and tactical air) of the United States and its allies are considered the prime deterrent to conventional military attack. Planning for the general purpose forces focuses on being able to defend Western Europe, while at the same time being able to conduct a lesser war in the Pacific theater. Again intelligence plays an important role in following the technical and force-level changes of potential enemies, and in predicting future trends. Current intelligence is also relied upon to provide adequate warning of the massive redeployment of men and materiel that would precede a conventional attack.

In the event of war, it will be critical to adapt the missions of the national intelligence-gathering systems to the needs of operational commanders. The planning for such contingencies poses a major challenge for leaders of the defense intelligence community.

The ongoing arms limitations negotiations on strategic and theater forces in Europe are guided by the principle of rough equality between opposing capabilities. Asymmetries in such factors as geography, technology, and manpower must be accommodated so that both sides believe there is an overall balance. Intelligence systems play a critical part in monitoring this balance since they are the only reliable means available for verifying the status of forces of potential adversaries. In fact, advances in technical intelligence collection systems have made the current arms limitation agreements feasible. Establishing compliance with the strategic arms agreements in force, as well as providing assistance in current negotiations, is now among the most vital missions of the national intelligence apparatus.

The technical capabilities of U.S. intelligence systems are probably now adequate to meet the demands of present agreements. Whether they can meet the needs of future agreements is unclear and dependent upon the specific terms negotiated. Some of the proposals advanced in connection with the Vladivostok Agreement and the Mutual and Balanced Force Reduction (MBFR) talks would test the abilities of current or envisioned intelligence systems to detect or verify with high confidence. Three of the most difficult enforcement areas which could arise under future agreements and which pose major problems for the intelligence community are:

—MIRV missiles which are concealed in silos or submarines;
—Cruise missiles whose launchers are easily concealed in bombers and submarines, and which may carry either conventional or nuclear warheads;
—Mobile forces and weapons (particularly nuclear systems) in Europe which can be transferred quickly to and from the theater, and are also readily concealed.

2. Evolution of Defense Intelligence Organizations

The complexities of modern defense have burdened the intelligence community with issues and responsibilities which could hardly have been anticipated when the United States emerged as the world's foremost military power three decades ago. In endeavoring to fill its expanding role in support of the nation's security interests, the defense intelligence apparatus has undergone periodic reorganization, generally leading toward more centralized management control. The desire to make the defense intelligence community more responsive to the needs of policymakers has motivated this trend.

At present, the most likely near-term prognosis is for a continuation of the general peace, interrupted at times by regional conflict and crisis, but not erupting into a major war or likely to involve direct U.S. military participation. The problem has been that in order to avert the big war, the U.S. has had to project a credible appearance of being able to win it, or, at least, not lose it decisively. This means it could not permit its war-fighting capacity, for which the military services hold the final responsibility, to erode unilaterally. Since the defense intelligence apparatus is a major contributor to that capacity, and since most of the important intelligence assets are operated by the armed forces, it is not surprising that the services have resisted efforts to channel these resources in different directions.

The existing organization of the defense intelligence community will be discussed in the following section. It is important to appreciate that it was not designed expressly to serve today's intelligence requirements or to manage today's intelligence functions. Rather, it should be perceived as basically a service to the military, adjusted through several decades of institutional compromise.

3. Early Beginnings

The first traces of U.S. military intelligence activities appeared in the Revolutionary War, when General George Washington, as commander of the colonial Army, recruited and trained a corps of intelligence agents to report on British activities. This effort, which included the use of codes, secret ink, and disguises, was short-lived, and the agents were mustered out of service with the rest of the Continental Army. Following Washington's precedent, commanders of U.S. military forces in later conflicts created *ad hoc* intelligence units on their own authority to serve their individual needs. Andrew Jackson had an intelligence operation in the War of 1812, and Winfield Scott had an intelligence unit in his command in the Mexican War. A number of the military commanders in the Civil War organized their own intelligence networks, and two autonomous organizations, both named the United States Secret Service, engaged in intelligence activities for the Union, although neither had any legal authority to operate.

In 1882, the Secretary of the Navy established an Office of Naval Intelligence to collect and record "such naval information as may be useful to the department in the time of war, as well as in peace."[1] This office developed a naval attache system to overtly collect information on foreign naval activities. It initiated a series of publications summarizing the information it had collected to keep the Navy abreast of foreign naval developments, and specifically provided the Naval War Board with information during the Spanish-American War.

The first comparable Army unit was the Military Intelligence Division of the Office of Adjutant General, established in 1885 to gather information on foreign armies. It, too, was active during the Spanish-American War, but by the outbreak of World War I the entire Division had shrunk to two officers and two clerks.

Both the Army and Navy greatly expanded their intelligence complements during World War I. The Army alone had more than 300 officers and 1,000 civilians engaged in intelligence work. In 1917, a War Department Cipher Bureau was created by administrative directive. This unit, sometimes referred to as the "American Black Chamber," solved more than 45,000 cryptograms (including one from the Sunday Times) and broke the codes of more than twenty nations. It was dissolved at the specific direction of Secretary of State Henry L. Stimson in 1929, who reportedly said: "Gentlemen do not read each other's mail."[2] This and similar measures left the service intelligence arms poorly prepared for World War II.

---

[1] A. P. Niblack, *The History and Aims of the Office of Naval Intelligence*, Division of Operations, United States Navy Department (Washington, D.C.: U.S. Government Printing Office, 1920).

[2] Herbert O. Yardley, *The American Black Chamber* (Indianapolis: Bobbs-Merrill, 1931), pp. 332, 348.

One of the first steps taken by President Roosevelt in the aftermath of Pearl Harbor was to order the creation of the Office of Strategic Services (OSS) in June 1942 under the direction of General William Donovan. During World War II, OSS, together with the Army and Navy intelligence organizations, was coordinated by the Joint Intelligence Committee of the Joint Chiefs of Staff.

A list of the functions of the principal OSS branches demonstrates the scope of its activity. The Research and Analysis section produced economic, military, social, and political studies, and estimates for strategic areas from Europe to the Far East; the Secret Intelligence group gathered information from within neutral and enemy territory; Special Operations conducted sabotage and worked with the various resistance groups; Counterespionage protected United States and allied intelligence operations; Morale Operations created and spread "black propaganda"; Operational Groups trained, supplied, and sometimes led guerrilla groups in enemy territory; the Maritime Unit conducted marine sabotage; and Schools and Training was in charge of the overall training and assessment of personnel, both in the United States and abroad. In addition, OSS was directed to plan and conduct such "special services as may be directed by the United States Joint Chiefs of Staff." Only Latin America, the FBI's bailiwick, and the Pacific Theater, General MacArthur's, were outside the OSS sphere of operations.

Jurisdiction over subjects of tactical military interest, such as order of battle data and enemy weaponry estimates, was left with the traditional service arms. OSS also did not prevail completely over other intelligence operations of the services, which achieved a number of notable wartime successes. Army Intelligence, for example, captured a high-level Nazi planning group in North Africa, obtained a map of all enemy minefields in Sicily, and captured the entire Japanese secret police force on Okinawa. Naval Intelligence, soon after United States' entry into the war, deduced the impending appearance of German guided missiles, such as the HS 293, the V-bombs, and homing torpedoes.

After World War II, President Truman issued an Executive Order abolishing the OSS on September 20, 1945. The Department of War absorbed some of its functions, such as the work of its Secret Intelligence group and of its Counterespionage program. The State Department assumed others.

The demise of the OSS did not, however, end the concept of a central intelligence organization. On January 22, 1946, President Truman established a National Intelligence Authority to advise him, and created a Central Intelligence Group to assist the NIA in coordinating national intelligence matters. These two organizations evolved, through the National Security Act of 1947, into the National Security Council and Central Intelligence Agency.

The rapid demobilization of the armed forces after the war, the creation of the first peacetime central intelligence organization, and President Truman's conviction that the military must be subordinated to civilian control were all factors which seemed to portend a diminished role for the armed forces within the post-war intelligence community.

The National Security Act of 1947, which created the CIA and NSC, also strengthened civilian authority over military services by drawing the War and Navy Departments together under a single Secretary of Defense. The new Secretary was given authority over all facets of the administration of the defense establishment. The identities of the Army and the Navy were preserved, however, under separate civilian secretaries who now reported to the Secretary of Defense rather than directly to the President. At the same time, the air elements of the Army were reformed under a new Department of the Air Force, with the same status as the two older service departments.

The broad powers granted the Secretary of Defense permit him to effect major organizational changes within the Defense Department by the simple expedient of issuing a directive. The Defense Intelligence Agency was created by such a directive in 1961. The Eisenhower administration had concluded in the late 1950s that a consolidation of the services' general (defined rather awkwardly as all non-SIGINT, nonoverhead, nonorganic intelligence activities) was needed, an idea which the Secretary of Defense in the new Kennedy administration, Robert F. McNamara, quickly endorsed.

The Joint Chiefs of Staff and Secretary McNamara disagreed on the form the new agency should take. The JCS were concerned with preserving the responsiveness of the service efforts to the military's tactical intelligence requirements. They therefore wanted a joint Military Intelligence Agency subordinate to them, within which the independence of the several military components, and hence their sensitivity to the needs of the parent service, would be retained.[3] McNamara wanted a much stronger bond. He was determined to utilize better the service assets to support policymakers and force structure planners, and to achieve management economies.

The Defense Intelligence Agency which emerged was a compromise. It reports to the Secretary of Defense, but does so through the JCS. The Joint Staff Director for Intelligence (the J-2) was abolished and replaced by the Director of the new DIA. The functions of the Office of Special Operations—the small intelligence arm of the Office of the Secretary of Defense (OSD)—were absorbed by DIA.[4] There has been continuing controversy among the services due to their reluctance to cede responsibilities to DIA because they feared downgrading wartime combat capabilities. Moreover, the OSD level of the Defense Department has pressed continuously for greater centralization; both of these controversies have hampered DIA throughout its existence.

Unlike the DIA, the National Security Agency (NSA) is a presidential creation. Established in response to a Top Secret directive

---

[3] Memoranda, from Secretary of Defense Robert McNamara to Chief, Joint Chiefs of Staff, Lyman Lemnitzer, 2/8/61; from Lemnitzer to McNamara, 3/2/61; from McNamara to Lemnitzer, 4/3/61; from Lemnitzer to McNamara, 4/13/61.

[4] Memorandum from Deputy Secretary of Defense Roswell Gilpatric to Secretaries of the Military Departments; Director of Defense Research and Engineering; Chief, Joint Chiefs of Staff; Assistant Secretaries of Defense; General Counsel; Special Assistant; and Assistants to the Secretary, 7/5/61; DOD Directive 5105.21, 8/1/61.

issued by President Truman in October 1952, NSA assumed the responsibilities of its predecessor, the Armed Forces Security Agency (AFSA), which had been created after World War II to integrate the national cryptologic effort. NSA was established as a separate agency within DOD reporting directly to the Secretary of Defense. In addition, it was granted SIGINT operational control over the three Service Cryptologic (collection) Agencies (SCAs): the Army Security Agency, Naval Security Group Command, and Air Force Security Service. Under this arrangement NSA encountered many of the same jurisdictional difficulties which were to plague DIA. In an effort to strengthen the influence of the Director of the National Security Agency (DIRNSA) over their activities, the SCAs were confederated in 1971 under a Central Security Service (CSS) with the DIRNSA as its chief. The mission of NSA/CSS is to provide centralized coordination, direction, and control for the United States Government's Signals Intelligence (SIGINT) and Communications Security (COMSEC) activities.

4. Current Organization

Describing the management structure of the Defense intelligence community would be a difficult task under the best of circumstances. Authority and influence within any big organization are often determined as much by personalities and working relationships as by formal chains of commands or job descriptions. For the sprawling and complex Defense intelligence network, the task is particularly challenging. Moreover, the community is in the midst of an executive branch-directed transition which may alter second-level management relationships throughout the Department of Defense. The executive branch has not yet revealed exactly what kind of structure it intends, if indeed its full reorganization plan has been decided.

Of necessity, the description which follows applies to the organization of the Defense intelligence community as it existed during most of 1975.[5]

As the Defense intelligence community is presently organized, the Secretary of Defense has three groups of assets: (1) the Defense agencies reporting directly to him, of which the National Security Agency, the Central Security Service, and classified national programs are the most significant (but also including the Defense Mapping Agency and the Defense Investigative Service); (2) the Defense Intelligence Agency, which reports to him through his principal military advisers,

[5] The most significant change apparently now being considered would affect the Office of the Assistant Secretary of Defense for Intelligence (ASD/I). This position is currently (as of April 1976) vacant. Reportedly, the duties of the ASD/I will be assumed by a new Deputy Secretary who will also have executive jurisdiction over the related fields of telecommunications and net threat assessment. In this case, the ASD/I position could be abolished. The possibility cannot be ruled out, however, that the executive envisions the new Deputy Secretary as an additional oversight position, in which case a new ASD/I reporting to him could be appointed. This is along the lines suggested by the Report to the President and the Secretary of Defense by the Blue Ribbon Defense Panel, July 1, 1970, on National Command and Control Capability and Defense Intelligence (hereinafter cited as the Fitzhugh Report, after its chairman, Gilbert W. Fitzhugh).

the Joint Chiefs of Staff, and is responsible for preparing Defense intelligence reports and estimates drawing upon the data collected by other arms of the intelligence apparatus; and (3) the intelligence arms of the individual military services under the immediate operational control of the service chiefs, which encompass the military's general intelligence collection agencies, their counterintelligence and investigative arms, and activities of tactical interest.

One of the largest organizations in the Defense intelligence community is the National Security Agency. Military personnel, facilities, and equipment play a predominant role in carrying out the mission described by NSA Director, General Lew Allen, Jr., in public session:

> This mission of NSA is directed to foreign intelligence, obtained from foreign electrical communications and also from other foreign signals such as radars. Signals are intercepted by many techniques and processed, sorted and analyzed by procedures which reject inappropriate or unnecessary signals. The foreign intelligence derived from these signals is then reported to various agencies of the government in response to their approved requirements for foreign intelligence.[6]

Other agencies reporting directly to the Secretary of Defense are concerned with more specialized subject areas than the cryptologic group and make smaller demands on resources. The Defense Mapping Agency is responsible for all defense mapping, charting, and geodetic activities. Although a substantial percentage of this Agency's activities are of vital intelligence interest, others are related only marginally to intelligence, and some have no defense connotation at all. Similarly, the Defense Investigative Service, responsible for carrying out background investigations, is generally not considered in the mainstream of the national intelligence effort.

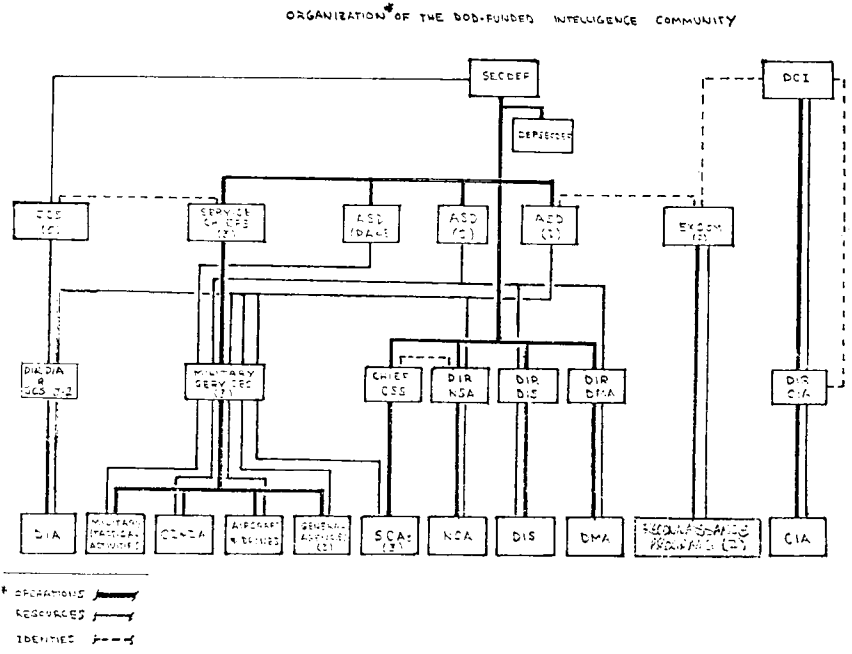
Aside from the Defense Investigative Service, each of the military services retains independent investigative arms responsible for both counterintelligence and criminal matters. These agencies fall within the ordinary military chain of command, and report to the Chief of Staff for each service. Other intelligence activities of national importance conducted under the uniformed services include the reconnaissance operations of Air Force aircraft and drones, and the general intelligence collection and analysis work of the U.S. Army Intelligence Agency, the Naval Intelligence Command, and the Air Force Intelligence Service. The service intelligence agencies are primarily oriented to supporting the tactical missions of the services, but they also collect information used by DIA in producing finished intelligence. The service agencies also continue to engage in activities related to national intelligence, and participate in the national estimates process as observers on the U.S. Intelligence Board.[6a]

A simplified diagram of the DOD-funded intelligence organization is presented on page 328. As is clear from the diagram, the organizational structure is extremely complicated, with several key individuals serving in more than one capacity, and disparate and diffuse chains of responsibility, both for deciding what is to be done and allocating the resources to do it.

---

[6] General Lew Allen, Jr., testimony, 10/29/75, Hearings, Vol. 5, p. 17.

[6a] USIB was abolished by Executive Order No. 11905, 2/18/76.



Perhaps the most significant feature of the above chart however, is what it does *not* show: a clear-cut line of authority extending from the highest councils of the executive branch to the operating arms of the intelligence apparatus. This is not surprising since this structure is the product of many years of bureaucratic evolution. Whether one views this arrangement as a crazy-quilt pattern, produced piecemeal over time in response to internal pressures, or as a finely balanced mechanism developed to meet needs as they arose, is largely a matter of perspective. It is hard to avoid observing, however, that if the apparatus has functioned even half as efficiently in allocating intelligence resources as its proponents maintain, it is because its participants have come to understand it well enough to make the system work in spite of itself. On the brighter side, the profusion of checks and balances inherent in the system may serve to reassure those who fear the potential evils of concentrating too much power in the hands of a single intelligence leader.

B. The Defense Intelligence Budget

1. Problems of Definition

The magnitude of national resources devoted to intelligence activities has recently been subject to considerable public speculation. Estimates of U.S. military intelligence spending have ranged from $3–4 billion annually to $15 billion, with most settling around the $6.2 billion figure cited in a recent book.[7]

[7] Victor Marchetti and John D. Marks, *The CIA and the Cult of Intelligence* (New York: Dell, 1974), p. 95.

Much of the controversy stems from definitions. What constitutes an intelligence activity? Which Government entities are intelligence organizations? Unfortunately, the budgeting practices of the intelligence community, and particularly the Department of Defense which controls the overwhelming bulk of intelligence resources, were not designed with much attention to functional clarity. Within DOD, institutional pressures to lower the "fiscal profile" of intelligence activities and rivalries over control of organizational assets have led to such discrepancies as placing the SR–71 program in the strategic forces account (Program I, a totally different section of the Defense budget).[8] Other examples of current budget practices are the exclusion of all communications security, counterintelligence, and mapping and charting activities from the Consolidated Defense Intelligence Budget (CDIB).

Although a case can be made that DOD's narrow definition of intelligence activities offers certain management expediencies in permitting the staff of the Assistant Secretary of Defense for Intelligence (ASD/I) to concentrate its attention on the central elements of the Defense intelligence effort, it produces such functional anomalies as the exclusion of important intelligence activities from the ASD/I's fiscal purview. Certainly, whatever degree of budgeting oversight the Congress elects to assume should address a fiscal presentation assembled on the basis of a more comprehensive definition of national intelligence activities than DOD uses at present.

Furthermore, a congressional oversight committee, in attempting to monitor DOD's counterintelligence budget, may want to group it with the counterintelligence budgets of all other intelligence agencies to provide management visibility to the national counterintelligence effort that is now lacking, even within the executive branch. Practical difficulties in distinguishing counterintelligence activities from ordinary criminal investigations (which, though totally different in purpose, are quite similar in method and often share common assets) should not be permitted to preclude an effort to establish a cross-agency grouping of the counterintelligence budget.[9]

The same problem of distinguishing intelligence and nonintelligence-related functions exists in the budgets for mapping and geodetic activities, most of which are the responsibility of the Defense Mapping Agency. Many of DMA's missions are only marginally related to the intelligence function, but others are of vital importance to all segments of the intelligence community's market. At a tactical military level, what intelligence commodity is of greater importance to a field commander than accurate maps of his area of operations? As with counterintelligence, the difficulties inherent in trying to separate the budgets of those facets of the mapping, charting, and geodetic effort which serve a national intelligence purpose from those

[8] The SR–71s were recently transferred from this category to the Strategic Forces (Program I in the Planning, Programing, and Budgeting System).

[9] The investigations for security clearances, previously a hodgepodge of disparate standards for uncoordinated, redundant efforts, were recently consolidated under a newly formed Defense Investigative Service (DIS). Nearly two-thirds of the budget for Counterintelligence and Investigative Activities (CI&IA) remains vested with the service agencies.

which do not should not be solved by the simple expedient of ignoring all such activities.

Still more difficult definitional problems arise when one probes more deeply the budgets of the armed forces in search of "tactical" as opposed to "national" intelligence functions. The difference between these two categories of intelligence lies in the eye of the consumer, not in the intelligence-collection activity itself. Increasingly, intelligence data-collection systems have grown capable of serving both the broad interests of the policymakers and defense planners and the more specific technical interests of the weapons developers and field commanders. In fact, a given set of collected data may often be of interest to all these groups, although the analytical slant with which it is presented is likely to differ markedly in response to consumer preferences.

There is an extensive gray area encountered in attempting to define military intelligence activities at the tactical or field command level. Many components of the military forces make a definite contribution to our intelligence effort during peacetime, but have other important missions as well, particularly during war. A prime example is the Navy's long-range, shore-based patrol planes, which play an important ocean surveillance role in peacetime, but would be an active part of U.S. antisubmarine warfare (ASW) combat forces during war. Although tactical military intelligence and related activities are included in the comprehensive cost estimates presented in the following section, the Committee believes the budgets of such activities should be excluded from the jurisdiction of a congressional intelligence oversight committee, with those committees in which it is currently vested retaining fiscal review authority.

The problem of reflecting costs of activities which are only partly intelligence-related in cost reporting is not confined to DOD. The diplomatic missions of the Department of State are responsible for political, economic, and commercial reporting, as well as normal representational and diplomatic responsibilities. The Department's Bureau of Intelligence and Research, which is both a consumer of intelligence and a producer of finished analyses, was budgeted for $9.5 million in FY 1976, of which 84 percent was spent on salaries. However, much more is spent each year to support State's embassies and consulates which, in addition to other duties, function in their political reporting activities as a human intelligence collection system. As with tactical military intelligence activities, the difficulties of trying to segregate the intelligence portion of the budget costs of these dual-purpose assets appear to outweigh the benefits.

2. The Size of the Defense Intelligence Budget in FY 1976

The Committee's analysis indicated that [deleted] billion [10] constitutes the direct costs to the U.S. for its national intelligence program for FY 1976. This includes the total approved budgets of CIA, DIA, NSA, and national reconnaissance programs.[10a] If the costs of tactical

[10] Deleted pending further Committee consideration.

[10a] Direct costs of the intelligence activities of the ERDA, FBI, and State Department are contained in their respective budgets.

intelligence by the armed services and indirect support costs [10b] which may be attributed to intelligence and intelligence-related activities are added in, the total cost of intelligence activities by the U.S. Government would be twice that amount. This represents about [deleted] percent of the federal budget, and [deleted] percent of controllable federal spending.[10c]

It should be stressed that this larger estimate represents a full cost and includes activities which also fulfill other purposes. Thus the entire amount could not be "saved" if there were no intelligence activities funded by or through the Defense Department.

A breakdown of the DOD intelligence budget divided by activity is shown in the table below. These estimates are based on a broader interpretation of what constitutes an intelligence activity than that used by DOD. The Department manages its national intelligence effort through the Consolidated Defense Intelligence Program (CDIP), and makes no formal effort to attribute indirect support costs. The summary includes only those activities funded through the Defense Appropriation Bill.

The costs of intelligence functions performed by the Departments of State (Bureau of Intelligence and Research), Treasury, Justice (Federal Bureau of Investigation), and the Energy Research and Development Administration (which has assimilated the intelligence division formerly operated by the Atomic Energy Commission) total about $0.2 billion.

Full Costs of Intelligence and Related Activities Within the DOD Budget: Fiscal Year 1976

(*In millions*)

Direct costs:	
Cryptology	-----
Communications security	-----
Reconnaissance programs	-----
Aircraft and drones	-----
Special naval activities	-----
Counterintelligence and investigation	-----
General intelligence	-----
Mapping, charting, and geodesy	-----
Central Intelligence Agency	-----
Subtotal, national intelligence effort	[deleted] [10d]
Strategic warning	-----
Ocean surveillance	-----
Tactical intelligence	-----
Weather reconnaissance	-----
Reserve intelligence components	-----
Subtotal, military intelligence effort	[deleted]
Total, direct costs	[deleted]
Indirect support costs:	
Basic research and exploratory development	-----
Logistics	-----
Training, medical and other personnel activities	-----
Administration	-----
Total, indirect support costs	[deleted]
Total, intelligence costs (budgeted by DOD)	[deleted]

[10b] Indirect support costs include costs for personnel, operations and maintenance which support intelligence activities. Examples are the operation of training facilities, supply bases, and commissaries.

[10c] Deleted pending further Committee consideration.

[10d] *Ibid.*

[DELETED]

3. Who Controls the Intelligence Budget?

The nominal head of the intelligence community is the Director of Central Intelligence (DCI), who is also the Director of the Central Intelligence Agency; these two roles, however, are to be viewed as distinct. A cornerstone of President Nixon's 1971 directive, designed

to foster the intelligence community's responsiveness to policymakers and promote management efficiency, was "an enhanced leadership role" for the DCI. Yet the DCI was not given direct authority over the community's budget, nor granted the means by which to control the shape of that budget until the announcement of President Ford's Executive Order of February 18, 1976.

As Director of the CIA, the DCI controls less than 10 percent of the combined national and tactical intelligence efforts. His chairmanship of the Executive Committees (ExComs), which oversee the management of certain reconnaissance programs (wherein he serves in what amounts to a partnership with the ASD/I), also affords him some influence over the funds budgeted for these efforts. The remainder spent directly by the Department of Defense on intelligence activities in FY 1976 was outside of his fiscal authority. The DCI's influence over how these funds are allocated was limited, in effect, to that of an interested critic.

By persuasion, he could have some minor influence, but the budgets themselves were prepared entirely within the Department of Defense. The small staff of the DCI may have been consulted in the process, but by the time it sees the defense portion of the national intelligence budget, the budgetary cycle has been well advanced, and hence the budget has been largely fixed. Problems of timing also influence the role of the Office of Management and Budget, which sets broad fiscal guidelines in budget ceilings, but plays an otherwise minor role in shaping the Defense intelligence budget.

The real executive authority over at least four-fifths of the total resources spent on intelligence activities has resided with the Secretary of Defense. Over the past few years, the Deputy Secretary of Defense has shown a particular interest in the intelligence portion of the DOD budget, in effect representing the Secretary on many issues arising in this area. However, the major responsibility for management of intelligence programs will lie with the newly created position of Deputy Secretary of Defense for Intelligence (Mr. Robert Ellsworth).

The Assistant Secretary of Defense for Program Analysis and Evaluation (ASD/PA&E) holds general review authority over the so-called mission forces, the operational forces which include much of the tactical intelligence assets of the military services. A third ASD, the Comptroller, is responsible for reviewing the budgets of the agencies concerned with counterintelligence investigations, and the newly formed Defense Mapping Agency. As explained earlier, DOD considers these activities peripheral to the intelligence effort, and their costs account for only about 5 percent of the overall intelligence budget.

The managers of the various intelligence programs collectively wield the greatest influence on day-to-day intelligence operations. By the

budget yardstick, the most influential individual is the Director of NSA (DIRNSA) who, including his dual role as Chief of the Central Security Service, manages the largest single program contained in the national intelligence budget, less than half of which is actually in the NSA budget.

Close behind the DIRNSA, and also directly related to the collection of signals intelligence data, is the United States Air Force in its role of managing certain reconnaissance programs. Decisions made regarding the introduction and development of reconnaissance systems have the greatest impact on the overall size of the intelligence budget, not only because of the direct costs of perfecting and procuring the hardware involved—as expensive as this technically complex equipment has become—but also because of the continuing effect that the choice of a collection system has on processing and other operating costs long after it has been made.

A third grouping of defense intelligence activities is the General Defense Intelligence Program (GDIP). In effect an "all other" category, the GDIP budget is ordinarily one-fourth Defense Intelligence Agency (DIA) costs, and three-fourths service costs (including those of the Air Force Intelligence Service, Naval Intelligence Command, and a part of the U.S. Army Intelligence Agency). The GDIP encompasses all of DOD's non-SIGINT, nonoverhead intelligence collection and production activities deemed by the Department to be of national importance. It does not include activities related to the military field commands.

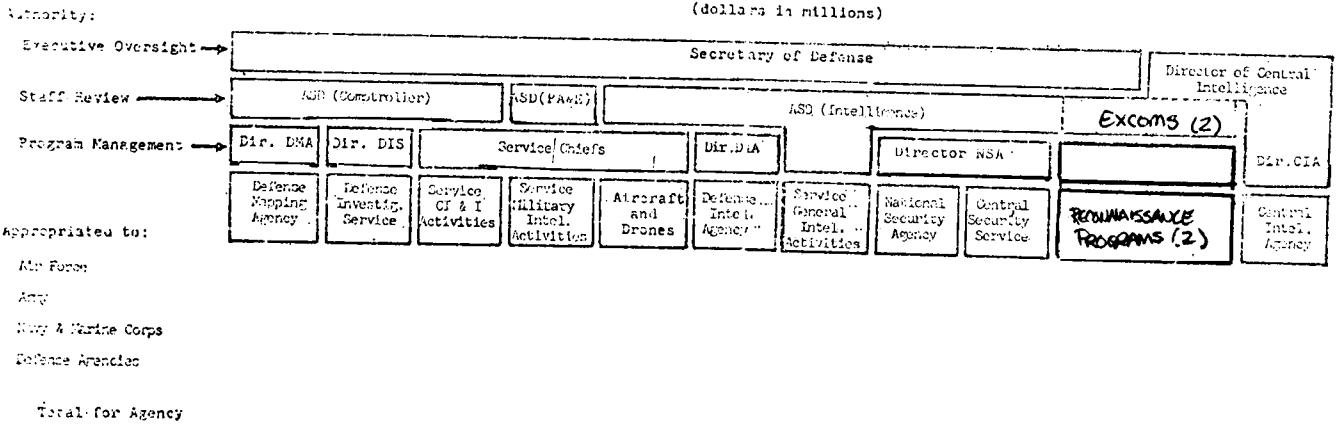
Although the general intelligence budget managed by the Director of DIA (DIRDIA) has never been more than a fraction the size of the DIRNSA's cryptologic budget, his problems, though similar, are more formidable. Whereas opinion is divided on the DIRNSA's grip over the service agencies that participate in the Consolidated Cryptologic Program (through the Central Security Service), there is little disagreement on the DIRDIA's inability to exert significant influence over the priorities and activities of the service components of the GDIP.

As a consequence, the program management responsibilities for the service general intelligence agencies previously held by the DIRDIA were recently transferred to the ASD/I. The result is that the DIRDIA, who purportedly still speaks for the Secretary of Defense on "substantive" matters within the intelligence community, exerts direct control over only 4 percent of the Secretary's intelligence budget.

The span of authority at each managerial tier—from executive oversight through fiscal review to program management—is summarized in the table on page 335.

Who controls the Intelligence Budget?
Distribution of the FY1976 Budget
Request by Organization and Recipient of Appropriated Funds

(dollars in millions)



[Figures deleted.]

Defense agencies each draw on resources funded within the service appropriations in addition to their own agency appropriations. These resources generally take the form of pay and allowances for military personnel who are serving tours outside their parent service with intelligence agencies. DIA's appropriation is supplemented by $39 million in this way; NSA's by $34 million; DIS by $16 million; and the Defense Mapping Agency's by $12 million. The Defense Department makes accounting corrections for these service-incurred costs in its Fiscal Year Defense Plan (FYDP), and the amounts are included in presenting the agency budgets. The important point to be recognized is that the budgets of the Defense intelligence agencies are not fully covered by the funds appropriated to them.

Slightly over a third of the overall DOD-funded intelligence effort is managed directly by the military services. The bulk of these funds support the tactical military requirements of the field commands and include many force components for which the intelligence mission is secondary or of shared importance with other activities. However, activities under service management are of national importance and interest in two areas: peripheral reconnaissance (carried out both by piloted aircraft, such as the SR–71, and unmanned drones), and counterintelligence and investigation (conducted by the Air Force Office of Special Investigations, the Naval Investigative Service, and a number of decentralized Army military intelligence groups).

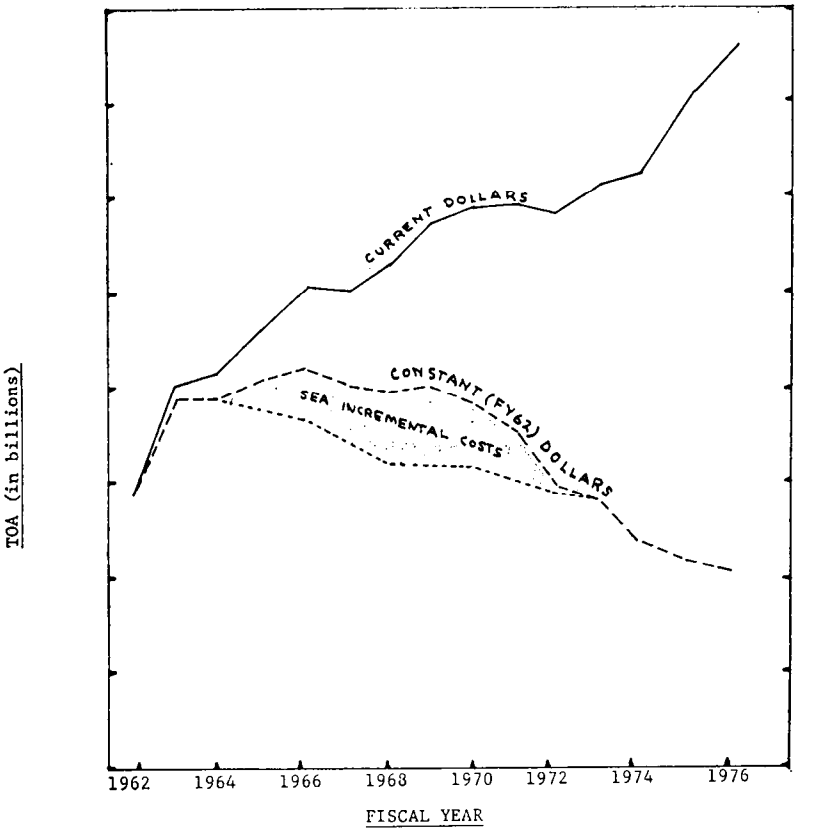
4. Budget Trends

The preceding section defined a [deleted] billion "package" of DOD-funded activities as a reasonable, comprehensive estimate with the addition of selected non-defense activities of a national intelligence budget subjected to separate congressional authorization. This section focuses on budget trends for this grouping of national activities.

In terms of simple dollar amounts, the FY 1976 DOD budget submission for national intelligence activities is the highest ever—over twice the amount appropriated in FY 1962. During periods of rapid inflation, however, "current dollars" are totally misleading as a measure of time trends in the consumption of real resources. Some allowance must be made for the year-to-year diminution in the purchasing power of a dollar that is brought about by rising prices. The method for doing so employs "price deflators" in an effort to express the worth of a series of heterogeneous "current-year" dollars in terms of the purchasing power of a dollar in some specific "constant" base year. The fact that these adjustments can seldom be achieved with precision does not negate their usefulness.

The chart on page 337 indicates the trends in the DOD-funded national intelligence budget (which includes the CIA as well as Defense agencies and the national activities of the military services) from fiscal year 1962 through fiscal year 1976. The upper, climbing curve plots current dollar amonuts as appropriated by the Congress except for fiscal year 1976, which is the amount requested by DOD. The lower, gradually descending curve shows the equivalent trend in the national intelligence budget after correcting, insofar as possible, for the effects of inflation by expressing each of the historical budgets in terms of the number of FY 1962 dollars it would take to purchase the same level of effort.

Trends in the National Intelligence Budget:
FY 1962-1976 a/



a/ Includes CIA budget. Does not include costs of tactical military intelligence activities.

After climbing rapidly during the first half of the 1960s, largely as a result of major program initiatives to acquire sophisticated reconnaissance systems (including the $1 billion SR–71 development program), the real "baseline" intelligence budget peaked at mid-decade at about [deleted] billion. Although outlay continued to grow moderately for several more years, the extra cost of supporting activities directly related to the war effort in Southeast Asia grew even more quickly, so that the amount available to support nonwar-related, or baseline, activities began to diminish. Since the mid-1960s, the budget has declined steadily, in terms of the resources that could be bought with the dollars provided, to the FY 1976 level of [deleted] billion, about equal in buying power to the budgets of the late 1950s.

A review of DOD planning documents indicates that every effort will be made by Defense leaders to avoid further erosion in the intelligence effort below the FY 1976 level Conversely, it is not anticipated that significant increases in funding (above those necessary to compensate for continued inflation, now expected to average 5–7 percent annually over the next five years) will be requested. If the Congress accepts these plans, a roughly constant level of real spending with gradually increasing annual appropriations to offset inflation can be expected.

Measured in today's prices, the budget request for Defense intelligence programs is also well below past funding levels: off $0.5 billion, or about 10 percent, from the FY 1962 level, and down nearly 30 percent from the pre-Vietnam peak of [deleted] billion. Compared to FY 1962, the largest reductions have taken place in the resources dedicated to some activities under NSA's management, which declined by 31 percent in real terms; and the development, procurement, and operation of reconnaissance systems, which went down 15 percent. Spending in support of aircraft and drone operations, although far below the peaks associated with the introduction of the SR–71, stands well above the level of 1962. Spending for communications security is also considerably higher today. Reflecting efficiencies achieved through the consolidation of independent service programs within the Defense Mapping Agency, real spending for mapping, charting, and geodetic activities is about $100 million less in FY 1976 than it was in FY 1962. Consolidation has also achieved economies in the field of counterintelligence and investigation, although on a far smaller scale. The $125 million requested for these activities stands about 15 percent below the pre-Vietnam level of effort.[11]

During the Committee's inquiry, informed managers within the Defense intelligence community frequently expressed the judgment that the downward trend in the resources dedicated to their programs has gone as far as it should. While acknowledging that no one has succeeded in devising a sound method by which to relate the value of the community's output to the quantity of resources used, they argue that most of the savings from the elimination of duplication and other forms of nonproductive effort have already been realized, and that further reductions can only be achieved at the risk of curtailing essential intelligence services.

5. How Much is Enough?

Because of the difficulties inherent in trying to quantify the intelligence community's output, no one has yet developed a rigorous method by which to relate the amount of intelligence produced to the amount of resources consumed in the intelligence effort. For this reason, it is not possible to state with confidence the effect that changes in the level of resources allocated to the intelligence mission could have on U.S. national security. In other words, no one really knows what comes out of the intelligence apparatus as a function of what goes into it.

The twin peacetime purposes for maintaining a national intelligence organization are to reduce the probability of key decisionmakers

[11] An estimated 20–40 percent of this amount will be spent for criminal, as opposed to counterintelligence, investigations.

making a wrong decision, either by taking inappropriate action in some matter important to U.S. interests or by failing to act at all, and to aid in assuring that U.S. Armed Forces are adequately prepared to execute decisions requiring military force. The intelligence apparatus is supposed to promote good policy and military readiness by making the policymakers and generals better informed than they might overwise be. However, the relationship between the quality of the information supplied to a national leader and the quality of the decisions made is obviously extremely complex and ill-defined. Although good intelligence may create a bias in favor of policymakers making good policy, it can offer no guarantees that such will transpire in every instance. All too easily, a bad policy judgment may be attributed to "intelligence failures."

If the level of effort were increased substantially, the quality of intelligence and national security would be enhanced. Conversely, substantial reductions could pose additional security risks. What cannot be ascertained with precision is whether the benefits would be worth the additional costs, or the savings the additional risks. At present, the issue can only be evaluated subjectively, taking into account those few factual statements that are at hand and the judgments of intelligence experts (recognizing, of course, the institutional biases the judgments may reflect).

On the one hand, the way in which the peacetime national intelligence budget has been shrinking has been duly documented. Apparently, these reductions have not significantly detracted from the overall performance of the national intelligence apparatus or seriously jeopardized U.S. security. Community managers interviewed during the Committee's investigation generally felt that present funding was adequate to provide all consuming groups with essential intelligence support. On the other hand, the same individuals were unanimous in their opposition to any further cuts in the budget—a view endorsed by the 1975 report of the Defense Panel on Intelligence, which stated: "We consider that the widely held concern over the inflated size of the intelligence effort is no longer valid." The report maintained that further "substantial" reductions should be contingent on one or more of the following:

—A conscious decision to modify intelligence priorities and coverage.
—The introduction of labor-saving devices (i.e., automation of the intelligence process).
—Reorganization of other management efficiencies.

In making the case against further reductions in the level of the national intelligence effort, it is commonly argued that the intelligence is labor-intensive (meaning that people, not machines, contribute the most to the community's product and account for the greatest share of its costs), and that the number of intelligence workers has declined sharply over the past several years. The community's managers contend that further personnel cuts should be made only as new equipment is introduced which can do more efficiently some of the tasks now performed by people.

The trend in defense intelligence manpower has been sharply downward: the fiscal year-end strength of 89,900 persons (civilian and military, U.S. citizens and foreign nationals) planned for 1976 is one-fifth less than that of fiscal year 1962, and 42 percent below the 1968 peak of 153,800 persons (some of whom were, of course, engaged in support of the Southeast Asia war effort). At the end of fiscal year 1975, 101,500 persons were engaged in defense national intelligence activities.

It is not true that the defense national intelligence effort is labor-intensive. Quite the opposite. Intelligence is highly capital-intensive; the defense intelligence community annually invests more per employee than the DOD-wide average.[12] As shown in Table 5, investment per man-year for the national intelligence sector of the Defense budget will average $16,700, about 11 percent less than was spent in 1962 despite the manpower reductions that have taken place, but still $2,800 more than will be invested by the general purpose forces at large, and only $1,800 less than the highly capital-intensive strategic forces. The downward trend in the investment rate for the intelligence components does not suggest a vigorous effort on the part of community managers to achieve the gains in efficiency through automation that they contend offer the best opportunity to realize further savings.

DEFENSE INVESTMENT RATES: FISCAL YEARS 1962–76

[Thousands of constant fiscal year 1976 dollars per man-year][1]

	1962	1964	1968	1972	1974	1975	1976	Percentage change, fiscal year 1962
Defense national intelligence components	18.7	22.0	15.3	14.8	14.8	16.3	16.7	−10.7
Strategic military forces	37.1	26.2	23.1	25.5	18.0	17.8	18.5	−50.1
General purpose military forces	12.1	12.4	[2] 15.9	[2] 13.1	12.1	10.0	13.9	+14.9

[1] Investment defined as sum of total obligational authority for associated RDT & E procurement and military construction. Average personnel strengths computed to include all military, U.S. civilian, and foreign national employees.
[2] These figures reflect increased investment in support of combat operations in Southeast Asia.

Lacking a sound methodology by which to relate outputs to inputs, management of the intelligence community must remain as subjective as the product in which it deals. The Committee did not receive the impression that the intelligence community was in fact striving to develop such a methodology, if indeed that is possible. The words of former Assistant Secretary of Defense Robert Froehlke sum up the existing situation lucidly: "The intelligence community does not know the minimum level of resources that will satisfy an intelligence requirement. There is no upper boundary set by requirements, only by the resources that are made available."

[12] The Department of Defense has requested $37.6 billion for investment (RDT&E, Procurement and Military Construction) in FY 1976 and will consume about 3.1 million man-years of labor for an average investment per man-year of $12,000. This compares favorably with the most capital-intensive sectors of U.S. manufacturing, such as petroleum and chemicals, and is many times greater than the investment spending of such truly labor-intensive industries as textiles.

C. Management Problems of the Defense Intelligence Community

1. Previous Studies

Senate Resolution 21's instructions that the Select Committee undertake a "complete investigation and study" to determine "whether there is unnecessary duplication of expenditure and effort in the collection and processing of intelligence information by United States agencies" strikes a familiar chord. Over the past decade, no fewer than six major studies have been commissioned within the executive branch to probe precisely the same question. Coinciding with the Congress' inquiry, another executive study of the community's organization was conducted, culminating in the actions taken by the President on February 18, 1976.

Earlier studies have not always agreed on details, but all have concluded that the defense intelligence community has performed neither as effectively nor as efficiently as possible, due largely to its fragmented organization. More centralized management control is needed if there is to be improvement in the cost-effectiveness of the community's efforts. Notwithstanding this view, the community's organizational structure has changed little over many years. Since many of the past studies of the community's organization have tapped greater resources than have been available to the Select Committee, the discussion which follows draws heavily upon their findings.

Writing in 1971 from his vantage point in the Office of Management and Budget (OMB), James R. Schlesinger compared the structure and management methods of the intelligence community to those of the Department of Defense prior to the Defense Reorganization Act of 1958. Obviously, this Act did not eradicate all of DOD's management problems. Similarly, reorganization of the intelligence apparatus could not in itself guarantee improved performance nor lowered costs. But reorganization could, in Schlesinger's view, create the conditions for inspired intelligence leadership. In his 1971 paper, Schlesinger concluded: "the main hope for improving cost-effectiveness did in fact lie in a fundamental reform of the intelligence community's decision-making bodies and procedures." [13]

In its letter of transmittal to the President, the 1970 Blue Ribbon Panel on Defense (the Fitzhugh Report), summed up its appraisal of the community's performance with the following criticisms:

> —Intelligence activities are spread throughout the Department of Defense with little or no effective coordination.
>
> —Redundance in intelligence, within reason, is desirable, and it is particularly important that decision-makers have more than one independent source of intelligence.
>
> —There is, as has often been charged, evidence of duplication between the various organizations.
>
> —There is a tendency within the intelligence community to produce intelligence for the intelligence community and to remain remote from and not give sufficient attention to the requirements of others who have valid needs for intelligence.

[13] Office of Management and Budget, "A Review of the Intelligence Community" (Schesinger Report), 3/10/71.

—There is a large imbalance in the allocation of resources, which causes more information to be collected than can ever be processed or used.
—Collection efforts are driven by advances in sensor technology, not by requirements filtering down from consumers of the community's products.[15]

The Blue Ribbon panel also cited the following allegations made by "responsible witnesses" during the course of its investigation, noting that there was no way to confirm or disprove any of the charges because there was no existing procedure to evaluate systematically the efficiency of the intelligence process or the substantive value of its output:

—The human collection activities (HUMINT) of the services add little or nothing to the national capability.
—Defense attaches do more harm than good.
—The intelligence production analysts are not competent to produce a sound, useful product.
—Once produced, the product seldom reaches the individuals who need it.

Each of these issues is discussed below.

2. Centralizing Management Controls

On this issue, the views of those who wish to avoid repetitions of past abuses by the community and those stressing the importance of improving the effectiveness and efficiency of the community's operations may not be compatible. Critics of centralization feel that reforms aimed at improving cost-effectiveness by concentrating budget and operational authority within the community might, at the same time, concentrate the power to undertake improper activities in the future. Centralization proponents counter that the diffusion of authority is as apt to encourage improper conduct as its concentration. A streamlined management structure would, they argue, promote the visibility and accountability of controversial programs.

If the Defense intelligence community were reorganized to promote more effective, centralized controls, what form might it take?

The office of the Assistant Secretary of Defense for Intelligence (ASD/I) has been the single most influential office in the preparation of the national intelligence budget under recent organizational arrangements. Although the ASD/I's authority is not absolute, he has more to say about how and where the national intelligence community invests its resources than any other individual by virtue of his fiscal review authority over the Consolidated Defense Intelligence Program (CDIP).

ASD/I was established largely as a result of a recommendation by the 1970 Blue Ribbon Defense (Fitzhugh) Panel, but it was not accorded the full authority the Panel proposed, and certain other complementary reforms were also not adopted. A classified supplement to the Fitzhugh Report called for creation of an ASD/I who would also serve as a new Director of Defense Intelligence (DDI).

[15] Fitzhugh Report, 7/1/70.

Under this arrangement, the same individual would have direct line authority over the operations of the DOD intelligence apparatus (via his position as Director of Defense Intelligence) and responsibility for review of resources allocated to it as Assistant Secretary of Defense for Intelligence.

The Blue Ribbon Panel further envisioned a reorganization of the DOD intelligence community along functional lines, separating collection and production activities into two new agencies, the heads of which would report to the ASD/I in his dual role as DDI.

Complementing its objective of creating a clear chain of command from the operating aims of the Defense intelligence establishment to the Department's top policymakers, the Panel also recommended the establishment of a Deputy Secretary of Defense for Operations who would represent the Secretary in all intelligence-related matters, and to whom the ASD/I–DDI would report directly. Although the recommendation to establish a second Deputy Secretary of Defense was not accepted in 1970, it is part of the 1976 executive reorganization plan.

3. Too Much Collection?

Numerous studies since the mid-1960s have concluded that a serious imbalance exists between the amount of data collected by the technical sensor and surveillance systems and the ability of the processors and analysts to digest and translate these data into useful intelligence information. These studies recommend that greater attention be given to producing better insights from the information and less to stockpiling data.

Analyzing the steep rise in the cost of intelligence activities during the 1950s and early 1960s, Schlesinger was among the first to blame the movement to employ ever more sophisticated technical collection systems, which he believed had led to "gross redundancies" within community operations. He concluded that the rapid growth in the collection of raw intelligence data was not a substitute for sorely needed improvements in analysis, inference, and estimation. The scope and quality of intelligence output, he concluded, had not kept pace with increases in its cost.

The Committee did not find any studies suggesting that more collection capacity is needed, although deficiencies in the responsiveness of existing collection systems have been frequently noted. Examples of general observations on overcollection are:

—Like the rest of the intelligence community, it (the CIA) makes up for not collecting enough of the right kind of information on the most important targets by flooding the system with secondary matter.

—The information explosion has already gotten out of hand, yet the CIA and the community are developing ways to intensify it. Its deleterious effects will certainly intensify as well, unless it is brought under control.

—The quantity of information is degrading the quality of finished intelligence.[16]

[16] "Foreign Intelligence Collection Requirements: The Inspector General's Survey." (hereinafter cited as the Cunningham Report). December 1966.

—Production resources can make use of only a fraction of the information that is being collected. There exists no effective mechanism for balancing collection, processing and production resources.[17]

The period of rapid growth in intelligence costs that undoubtedly motivated much of the concern about overcollection has passed. Although the level of total real spending has now returned to what it was during the late 1950s, the efficiency with which intelligence resources are being apportioned among the collection, processing, and production functions remains an issue.

An examination of the distribution of the national intelligence budget dollar in FY 1975 indicates that most of the community's resources support collection activities. The community is still spending 72 percent of its funds for collection, 19 percent for processing raw technical data, and less than 9 percent for the production of the finished intelligence products (bulletins, reports, etc.) which the consumer sees as the community's output. There has been no significant change in the allocation over the past several years, nor is any anticipated.

The collection of unused information results in greater inefficiencies than merely the effort wasted on collection. Backlogs in processing and analysis lead to duplicative efforts across the board, since the results of preceding collection missions are not always available to plan and manage current missions. Moreover, the rush to keep pace with the data disgorged by the technical collection systems encourages superficial scanning, increasing the probability that potentially important pieces of information will be overlooked.

4. Alternative Means of Collection

There are major disagreements within the community between proponents of traditional collection methods employing undercover agents (human intelligence, or HUMINT) and advocates and operators of the vast system of technical sensors. Approximately 87 percent of the resources devoted to collection is spent on technical sensors, compared to only 13 percent for HUMINT (overt and clandestine operations).

Most of the intelligence experts interviewed during the Committee's inquiry tended to endorse the existing seven-to-one distribution of resources in favor of technical collection, but the efficacy of the technical sensors was not unanimously acclaimed. Deputy Secretary of Defense William P. Clements, Jr. commissioned the Defense Panel on Intelligence (1975)[18] largely because of his concern with the failure of the analytical community to alert national leadership to the October 1973 Middle East war.

The Defense Panel Report stressed the importance of upgrading HUMINT, noting: "We are not getting [as of 1975] the level or quality of information we need from this source."[18] The Report credited the CIA's Clandestine Service as the most competent U.S. HUMINT collectors, but held this arm was not very responsibe to DOD needs. It

[17] Fitzhugh Report, 7/1/70.
[18] Report of the Defense Panel on Intelligence, 1/75.

was concluded that the principal Defense HUMINT collectors, the Defense Attaché System (DAS) managed by DIA, were yielding valuable returns at small cost, but greatly needed a personnel upgrading. Other critics have been less charitable to the attaches.

The problem of measuring intelligence output prevents accurate assessment of the contribution of different collection methods. Shifts in the uses of intelligence systems among peacetime, crisis, and wartime situations further complicate appraisals, as does the divergent interests of the national and tactical consumer groups. Civilian policymakers tend to plan for peacetime situations, whereas military commanders envision quite different wartime demands on the intelligence apparatus. The shifts of importance between peacetime and wartime are illustrated by the fact that much of the economic intelligence collected today would be accorded a much lower priority during a major war. Similarly, the verification of arms control agreements, now a major intelligence task, would be moot after the outbreak of hostilities between the major powers.

Against this backdrop, only an approximate evaluation of the comparative worth of the various methods of intelligence collection has been possible for the Committee. The results of such an evaluation are summarized as follows:

Performance was judged against two criteria: the ability of the method to accomplish specified intelligence objectives, and characteristics deemed desirable in intelligence systems.[19]

The analysis indicated that reconnaissance programs and SIGINT systems rank high in characteristics and performance. Not surprisingly, their costs are also the highest of all the competing systems.

HUMINT did not score as highly as might be expected, based on the emphasis and funds accorded to this activity. Still, overall, the evaluation indicated that a fairly good correlation exists between the benefits achieved by collection activities and their costs.

The priorities for spending among different collection systems appear to be appropriate. This does not mean that there is no need for adjustment in the pattern of resource allocation for collection methods. A major analytic effort on the part of the community offers the only means for achieving such efficiencies.

Although the issue of proper balance between collection, processing, and production is usually phrased in terms of overcollection, it might also be described as a problem of underproduction. Deputy Secretary of Defense Clements stated: "In every instance I know about where there was a horrendous failure of intelligence, the information was in fact available to have averted the problem. But the analysts and the system didn't allow the raw data to surface." [20]

---

[19] The following intelligence objectives are considered: strategic warning; crisis indication; foreign weapons development; foreign military deployments; political and military intent; economic information; political information; tactical military information.

The following characteristics were considered: ability to penetrate denied areas; accuracy and reliability of data; responsiveness; wartime survivability; peacetime risks of incident.

[20] Quoted by William Beecher in Report of the Defense Panel on Intelligence, 1/75.

Similarly, the Defense Intelligence Agency, the arm of the Defense Department charged with the prime responsibility for intelligence analysis and production, concluded in a 1973 report:

> The great disparity in the relative national investment in collection systems versus intelligence processing, exploitation, production and support systems has now reached a platitude [*sic*] where the anticipated payoff of a high cost collection system is limited by the DIA's capability to exploit them [*sic*] fully.

If production is the limiting step in the intelligence sequence, improved overall efficiency might be achieved by enhancing this capacity as well as by cutting back on collection. It is not clear, however, that the DIA's suggestion to spend more on production, implied in the above passage, would solve the largely qualitative shortcomings now limiting the performance of some intelligence producers.

5. Setting Intelligence Priorities

Intertwined with the issue of how much should be spent on intelligence activities is the question of how best to spend it. This poses a whole series of complex, interrelated choices ranging from subject matter to "line balance" (i.e., synchronizing the collection, processing, production, and dissemination among methods and means of collection).

The most critical resource allocation choices concern the subjects and geographic areas against which the community should target its energies. Logically this choice would reflect the changing interests of intelligence consumers, weighted according to national importance. Lower-order choices, such as the design and selection of a new technical collection system, would be made in order to meet consumer demands.

Unfortunately, the system does not work this way. Although expressed with varying degrees of forcefulness, almost every previous study of the management problems of the national intelligence community has agreed that the formal mechanism for establishing priorities to guide the community's allocation of resources (i.e., the so-called requirements process) works poorly, if at all. In his 1968 report to the Director of CIA regarding the actions taken in response to the recommendations of the Cunningham Report, Vice Admiral Rufus Taylor put the problem this way:

> After a year's work on intelligence requirements, we have come to realize that they are not the driving force behind the flow of information. Rather, the real push comes from the collectors themselves—particularly the operations of large, indiscriminating technical collection systems—who use national intelligence requirements to justify what they want to undertake for other reasons, e.g., military readiness, redundancy, technical continuity and the like.

The Schlesinger and Fitzhugh reports concluded that the focus of the community's efforts is determined by the program managers and operators of the highly complex technical collection systems that dominate the community's budget, rather than by the priorities of the intelli-

gence consumers. Schlesinger called the formal requirements "aggregated wish lists" that could be interpreted as meaning "all things to all people," thereby creating a vacuum which left the individual intelligence entities free to pursue their own interests. The Blue Ribbon Panel noted that no effective mechanism existed for consumers, either national or tactical, to communicate their most important needs.[21] Requirements, concluded the Panel, "appear to be generated within the intelligence community itself."

In 1960, before major developments in data collection, a joint study group criticized the requirements process and recommended sweeping changes in the system. Six years later, the Cunningham Report described the principal instrument in the requirements process, the Priority National Intelligence Objectives (PNIOs), as a "lamentably defective document which amounts to a ritual justification of every kind of activity anybody believes to be desirable," wryly adding, "We found no evidence that an intelligence failure could be attributed to a lack of requirements."

Poor communication between the producers of intelligence and the consumers continues to be the greatest obstacle to improved efficiency in the use of the community's resources.

6. Resource Allocation

Without judging the appropriateness of the community's subject or geopolitical emphases, a brief description of the way in which resources have been allocated follows.

In FY 1975, more than half the community's effort, about 54 cents of each dollar, was targeted against military subjects such as doctrine, dispositions, force levels, and capabilities. Twelve times more effort went into collecting and processing information of this kind than toward analyzing it. For technical and scientific subjects, the effort was divided in the ratio of six parts collecting and processing to one part analysis. Only about six cents on the dollar was focused on either political or economic subjects. Resource allocation by subject and function is shown in the table below.

NATIONAL INTELLIGENCE PRIORITIES

DISTRIBUTION OF THE FISCAL YEAR 1975 INTELLIGENCE DOLLAR BY SUBJECT[1]

	Collection	Processing	Production	Total
Subject area:				
Military	41.4	8.3	4.1	53.8
Scientific and technical	11.4	1.8	2.3	15.5
Political	2.5	.3	.6	3.4
Economic	2.2	.3	.7	3.2
General	14.9	8.3	.9	24.1
Total, fiscal year 1975	72.4	19.0	8.6	100.0
Total, fiscal year 1974	71.8	19.5	8.7	100.0
Total, fiscal year 1976 (requested)	72.4	19.1	8.5	100.0

[1] Based on the budgets of the Central Intelligence Agency, the State Department's Bureau of Intelligence and Research, and that portion of the Defense Department's budget included within the Consolidated Defense Intelligence Program (CDIP). This does not include mission support costs.

[21] Two separate consumer priority polls, one undertaken by the staff of the DCI, the other by the DIA, were explained to the Committee. In neither instance was there evidence that the study had produced a significant or lasting impact on management practices.

A second important way in which the existing priorities of the national intelligence community are revealed is through the distribution of spending across the geopolitical spectrum. There is little doubt that the most formidable potential threat to the United States is posed by the Soviet Union, with the second most dangerous potential military antagonist being the People's Republic of China. Most analysts would also hold that the nation's foremost commitment overseas is to the defense of its NATO allies. Vital interests in Asia include the security and pro-Western orientation of Japan and the defense of the Republic of Korea, to which the United States has had long-standing treaty commitments. Instability in the Middle East, to a lesser degree South America, and for the moment in Africa, would seem to argue for special attention to these areas as well.

The attributable portion of the FY 1975 intelligence effort was distributed among different target areas as follows: nearly two-thirds of the resources consumed, 65 cents of each dollar, were directed toward the Soviet Union and U.S. commitments to NATO; 25 cents of each dollar were spent to support U.S. interests in Asia, with most of this targeted against China; the Arab-Israeli confrontation in the Middle East claimed seven cents; Latin America, less than two cents; and the rest of the world, about a penny.

7. Management Efficiency versus Security

In addition to the issues of balance in meeting the demands of both national and tactical consumers, and in the distribution of resources among the collection, processing, production, and dissemination functions in the intelligence sequence, there is also an issue of balance in the flow of information. Here the opposing considerations are security and management efficiency. There is a legitimate need to protect both what is known about a potential adversary's capabilities and the way in which the knowledge was acquired.

The Committee's investigation surfaced considerable sentiment that the community's preoccupation with compartmented security may have reached a point where communications are so restricted that effective analysis and dissemination of intelligence is impaired. The Cunningham Report observed: "Some [intelligence] tasks require piecing together many bits of information to arrive at an answer. Compartmentalization hinders cross-discipline cooperation."

Supporters of the community's existing security arrangements counter that few analysts with a proven "need to know" are denied the clearances necessary to gain access to the information they require. Yet the problem is more subtle than this. Merely allowing the diligent analyst to acquire information is not enough. Kept in ignorance of certain subject areas by the compartmentalization system, it is difficult to determine which particular security barriers to storm in search of that last, missing fact that could unlock the puzzle with which the analyst is grappling.

The Cunningham Report also noted a "real need to make comparisons and tradeoffs between intelligence activities and programs to select the most efficient systems," a need which the Committee believes to be unmet today, despite organizational changes. The manager constrained to a narrow view by the blinders of compartmentalization is hardly in the best position to make such tradeoffs.

D. Agencies and Activities of Special Interest

1. The Defense Intelligence Agency

Formally established in August 1961 by Department of Defense Directive 5105.21, the Defense Intelligence Agency (DIA) was envisioned by its civilian proponents as a means of achieving more centralized management control, thereby leading to a "more efficient allocation of critical intelligence resources and the elimination of duplicating facilities and organizations." [23] The Agency was granted full authority for assembling, integrating, and validating all intelligence requirements originating with the Department of Defense, setting the policy and procedures for collecting data, and developing and producing all finished defense intelligence products.

Currently, the Agency is organized into five directorates, each headed by a Deputy Director. The Directorate for Estimates produces all DOD intelligence estimates, including DOD contributions to National Intelligence Estimates (NIEs) for the National Security Council, as well as forecasts in the areas of foreign force structures, weapon systems, deployments, and doctrine. The Deputy Director for Estimates is also responsible for coordinating with CIA, State, and NSA on intelligence estimates, and assisting these agencies with information on military capabilities and strategies.

Intelligence assessments of special interest to military forces in the field are the responsibility of the Directorate for Production. Other directorates specialize in determining foreign technological progress and the performance of foreign weapon systems (the Directorate for Science and Technology); coordinating service requests for intelligence information (the Collection Directorate); and administering the Defense Attache System (the Directorate for Attaches and Human Resources).

The national leaders who established the DIA were alert to the danger that it might evolve into simply another layer in the intelligence bureaucracy, and cautioned against thinking of it as no more than a confederation of service intelligence activities.[24] Nonetheless, a decade later executive branch reviews criticized DIA for perpetuating the very faults it had been designed to avoid—duplication and layering.[25] By 1970, each service actually had a larger general intelligence arm than it had had before DIA was created. At that time, the Blue Ribbon Defense Panel reported:

> Each [military] departmental staff is still engaged in activities clearly assigned to DIA such as intelligence production including the preparation of current intelligence. The Military Departments justify these activities on the basis that DIA does not have the capability to provide intelligence they need. It is interesting that DIA cannot develop a capability to peform its assigned functions, while the Military

---

[23] Press release accompanying the creation of DIA, cited in the Froehlke Report, 7/69.

[24] Gilpatric memorandum to Joint Chiefs of Staff, 7/1/69.

[25] Fitzhugh Report, Appendix: "National Command and Control Capability and Defense Intelligence," 1970, pp. 33-34; William Beecher, Report of the Defense Panel on Intelligence, 1/75.

> Departments, which provide a large proportion of DIA personnel, maintain the required capability and continue to perform the functions.[25a]

In trying to integrate massive and disparate defense intelligence requirements, DIA had become increasingly bogged down in management problems, notwithstanding a number of internal reorganizations in search of the right mechanisms of coordination. At the root of the DIA's difficulties lie the opposing pulls from Washington-level civilian policymakers, who demand broad insights of a largely political character, and military planners and field commanders, who require narrower and more specific factual data. DIA has never really known which of these groups of consumers comes first. As the Fitzhugh Report stated: "The principal problems of the DIA can be summarized as too many jobs and too many masters."

In retrospect, a strong case can be made that the DIA has never really had a chance. Strongly resisted by the military services, the Agency has been a creature of compromise from the outset. For example, the Director of the DIA was placed in a position of subordination to the Joint Chiefs of Staff (JCS) by designating him to serve as the JCS director for intelligence (replacing the J–2 on the Joint Staff). Drawing again from the Fitzhugh Report, this arrangement put the Director of DIA in the "impossible position" of providing staff assistance on intelligence matters to both the Secretary of Defense and the JCS, whose respective stances on a given issue "often are diverse."

DIA was also reliant on the military for much of its manpower which was initially drawn almost entirely from the intelligence arms of the various services. The argument for manning the new DIA with these personnel was to minimize the disruptive effects of organizational change on the flow of intelligence information. This same case was made for starting the DIA slowly. As a consequence, the Agency never had the impetus which many other newborn government entities have enjoyed and profited from. Dominated and staffed in large part by the professional military, it is not surprising that DIA has come to concentrate on the tactical intelligence demands of the services and their field commands.

Since DIA has always been heavily staffed with professional military officers on short tours, who are dependent on their parent services for future assignments and promotions, the perspective of Agency analyses has often been biased to reflect the views of the services. When evidence is doubtful, the services have incentives to tilt an intelligence appraisal in a direction to support their own budgetary requests to justify existing operations and proposed new ones.[28] Intelligence issues in the Vietnam war reflected this problem.

On the budget side of the problem, the Agency has been limited in its ability to control the activities of the services by the lack of follow-

---

[25a] Fitzhugh Report, pp. 23, 31–32.

[28] Harry Howe Ransom, *The Intelligence Establishment* (Cambridge, Mass., Harvard University Press, 1971), p. 103; Department of Defense, *The Senator Gravel Edition: The Pentagon Papers*, Vol. IV (Boston: Beacon Press, 1971); Patrick J. McGarvey, *CIA: The Myth and the Madness*, pp. 149, 134; *Pentagon* Papers, passim; Chester Cooper, "The C.I.A. and Decision Making," *Foreign Affairs*, January 1972.

up authority over intelligence activities: "Once money to support the approved program is allocated to the services, they may or may not use it for its intended purposes." [29] In an effort to remedy this, program management responsibilities over service components of the General Defense Intelligence Program (GDIP) were recently transferred from the Director of DIA to the ASD/I.

The services' concern with autonomy and preservation of wartime capabilities may make the achievement of any appreciable reduction in duplicative effort an impossible goal, at least for general intelligence activities. The problem is not simply one of bureaucratic pettiness; there exist unavoidable trade-offs between tactical and national intelligence interests. The issue of which set of needs should dominate Defense intelligence is a difficult one, with past disagreements on this point having played a major part in the dissatisfaction with DIA that has been expressed by the services, policymakers, and OSD staff.

The jurisdictional dilemma was recognized by Schlesinger in his 1971 report: "If the services retain control over the assets for 'tactical' intelligence, they can probably weaken efforts to improve the efficiency of the community. At the same time there is little question about their need to have access to the output of specified assets in both peace and war." He cited service resistance to the National Security Act of 1947, and to the 1961 DOD Directive establishing the DIA, concluding: "Powerful interests in the military opposed, and continue to oppose, more centralized management of intelligence activities."

A second factor contributing to the dissatisfaction frequently expressed by DIA's customers has been the quality of the Agency's analysis. Most often, this is perceived as a problem of professional competence.

Illustrating the deficiencies in intelligence production as viewed by policymakers, Beecher has quoted former Secretary of Defense Schlesinger: "when you have good analysis, it's more valuable than the facts on a ratio of ten to one. But all decisionmakers get are factual 'snipets.' " Such tidbits, while often interesting in content, are of limited worth if not woven into context. The "analyst" who serves as no more than a conduit for transmitting facts is not providing analysis. Yet, the job of the national intelligence analyst is to sort facts, discarding those which do not appear relevant, and piecing together what remains in a way that yields the broad insights policymakers find most useful.

Besides a thorough understanding of his subject, the competent analyst must possess the qualities of perception, initiative, and imagination. Equally important, the analyst must be kept highly motivated and must be permitted, on occasion, to be wrong. (This is the basis of the argument for maintaining more than one source of key intelligence estimates.)

Critics have often commented harshly on the quality of both civilian and military personnel in DIA.[30] There are two facets to the problem of obtaining first-rate analysts: On the military side, capable and ambitious officers have traditionally avoided intelligence assignments,

---

[29] Fitzhugh Report, p. 23.

[30] e.g., *Ibid.*, p. 29; "Defense Panel on Intelligence," p. 6; McGarvey, *CIA: The Myth and the Madness, passim.*

deeming such positions not conducive to career advancement. Of the officers who have gone into intelligence, many of the best qualified have tended to serve with their individual service agency rather than joining DIA. DIA's leadership maintains, however, that gains have been made in correcting service biases in the intelligence career field. Since 1974, promotion prospects for officers in the service intelligence agencies have become equal to or better than the service-wide averages. This offers scant consolation for DIA, however, since the promotion rates for attachés and Navy and Air Force officers serving with the Agency have not improved proportionately, and remain less favorable than the service averages. There are, in fact, some indications that promotion prospects for officers at DIA may be deteriorating.[31]

On the civilian side of the personnel problem (about 55 percent of the DIA's 2,700 professional-level employees are civilian), it is frequently argued that a predominance of military officers in middle-management positions limits advancement opportunities within the Agency for civilian professionals. In addition, a significant portion of those "civilian" personnel who have reached management ranks are in fact retired military officers.

Many experts who have studied the DIA's personnel problems have concluded that improvement in the competence of the Agency's civilian analysts is contingent upon a relaxation of the constraints imposed by Civil Service regulations. The 1975 Report of the Defense Panel on Intelligence commissioned by Deputy Secretary of Defense Clements, asserted: "The professionalism of the intelligence production process must be improved substantially," and it strongly recommended exempting DIA's analysts from the Civil Service.

Whether exempting civilian professionals from the Civil Service and increasing their management presence would bring about the changes required to transform the DIA into an effective competitor to the CIA in producing national intelligence estimates remains questionable. The DIA has a problem of image. It is a problem that calls for fundamental reform of its management attitudes and orientation, as well as in its professional staffing. In the absence of the complementary reforms,[32] it would seem doubtful that the provision of greater incentives for its civilian analysts, and greater management latitude for the hiring and firing of these analysts by removing Civil Service constraints would in itself suffice to bring about the needed degree of improvement in performance.

Moreover, data on the civilian grade structure of DIA, compared to that of the CIA, suggest that far too much emphasis may be placed on the need to raise the salaries of DIA's civilian analysts. Conventional wisdom holds that the CIA has outperformed the DIA because its superior grade structure permits it to attract and retain more capable analysts. In fact, however, there is no significant difference in the professional grade structure (defined here as GS–9, or equivalent, and above) of the two agencies.

---

[31] Memorandum from Vice Admiral DePoix to Secretary of Defense Schlesinger, 3/4/74. Memorandum from Lt. Gen. Graham to Schlesinger, 11/19/74.

[32] Such as a new headquarters facility—a request that has been repeatedly denied by the Congress, but is an essential first step if a revitalized DIA within the existing organizational structure is decided upon as the preferred course of action.

About one-third of the upper management positions at DIA are filled by military general officers, a much larger proportion than at the CIA, where fewer military personnel serve.

Criticism of the professional standards of DIA's personnel has not been restricted to the Agency's managers and production analysts. The Defense attachés, who serve under the Agency's direction as the Defense Department's human intelligence (HUMINT) collection arm, have also been a topic of considerable concern. One 1970 study of the Defense Attaché System warned that the representational and protocol responsibilities of attachés were assuming precedence over intelligence functions which should constitute the principal purpose of the attachés.[33] This preoccupation with nonintelligence activities remains strong today.

The qualifications of the officers assigned to attaché duty have been questioned. The chances for promotion have usually been low in DAS and the tendency has been to draw a high proportion of attachés from among officers on their last tours before retirement. Former DIA Director Donald Bennett dismissed 38 attachés outright for incompetence when he took over the Agency in 1969.[34]

The arguments cited above suggest two basic alternatives for the Defense general intelligence apparatus: either retain the current centralized arrangement under the Defense Intelligence Agency, giving its Director the authority he needs to fulfill his original mandate to manage all of DOD's intelligence collection and production activities, or disband the Agency, returning its resources to the military services from which they were originally requisitioned, leaving the coordination of the tactical military aspects of these activities to the JCS, and forming a staff close to the Secretary of Defense to produce the national intelligence estimates he requires.[35]

There should either be a major role for DIA, or for the service agencies, but not for both, unless they genuinely serve different functions. Duplication of intelligence analyses can be valuable if it promotes diversity and motivates through competition. This assumes that the separate analysts have different perspectives on the issues. In this sense, competition between CIA analysts and Defense Department analysts for strategic estimates, is very useful. By arguing different points of view in forums in the intelligence community they force disagreements to the surface and expose evaluations to closer scrutiny. DIA now has had little incentive to serve as a CIA-type foil to the services, since DIA has been primarily a military organization.

Specific measures which might improve the performance of DIA within the existing organizational structure include the following:

a. Enhance professional competence.—Exempt DIA from Civil Service regulations in the same manner as CIA and NSA. Open more top-level jobs within DIA to civilian staffers. Increase incentives for the military services to send better qualified officers to DIA. Waive seniority requirements for Defense Attachés. Rotate DIA and CIA strategic analysts through each agency on temporary tours.

---

[33] Report of the DIA Defense Attaché System Review Committee, 5/30/70, pp. II–1, II–2.

[34] Staff summary of Lt. Gen. Donald V. Bennett, USA (ret.) interview, 7/23/75.

[35] A nucleus for which already exists in the Office of Net Threat Assessment.

b. Increase the responsiveness of the Agency to the Secretary of Defense and his staff.—Give ASD/I (or the new Deputy Secretary) authority to deal with the substance of intelligence programs as well as the allocation of resources. Have the Director of DIA report directly to the Secretary of Defense, rather than through the JCS, as under the present arrangement. Appoint a civilian as either the Director or Deputy Director and make the Director subject to Senate confirmation.

c. Increase DIA's management authority to match its management responsibility.—Allow DIA to establish more requirements for the service intelligence agencies, and to eliminate intelligence products of the military services which are unnecessarily duplicative.

d. Increase lateral communication between DIA and other components of the defense intelligence apparatus.—To integrate better the work of the operators, analysts, and planners, encourage communication among DIA regional analysts and desk men in CIA, ISA, and other policy staff offices in DOD and State.

2. The National Security Agency

The National Security Agency/Central Security Service (NSA/CSS) provides centralized coordination, direction, and control of the Government's Signals Intelligence (SIGINT) and Communications Security (COMSEC) activities.

The SIGINT or foreign intelligence mission of NSA/CSS involves the interception, processing, analysis, and dissemination of information derived from foreign electrical communications and other signals. SIGINT itself is composed of three elements: Communications Intelligence (COMINT), Electronics Intelligence (ELINT), and Telemetry Intelligence (TELINT). COMINT is intelligence information derived from the interception and analysis of foreign communications. ELINT is technical and intelligence information derived from electromagnetic radiations, such as radars. TELINT is technical and intelligence information derived from the interception, processing, and analysis of foreign telemetry. Most SIGINT is collected by personnel of the Service Cryptologic Agencies located around the world. The Director, NSA/Chief, CSS has authority for SIGINT missions.

The COMSEC mission protects United States telecommunications and certain other communications from exploitation by foreign intelligence services and from unauthorized disclosure. COMSEC systems are provided by NSA to 18 Government departments and agencies, including Defense, State, CIA, and FBI. The predominant user, however, is the Department of Defense. COMSEC is a mission separate from SIGINT, yet the dual SIGINT and COMSEC missions of NSA/CSS do have a symbiotic relationship, and enhance the performance of the other.

A specific National Security Council Intelligence Directive (NSCID) defines NSA's functions. It is augmented by Director of Central Intelligence Directives (DCIDs) and internal Department of Defense and NSA regulations.

NSA responds to requests by other members of the intelligence community, such as CIA, DIA, and FBI, to provide "signals" intelligence on topics of interest. An annual list of SIGINT requirements is given to NSA and is intended to provide the NSA Director

and the Secretary of Defense with guidance for the coming year's activities. These requirements are usually stated in terms of general areas of intelligence interest, but are supplemented by "amplifying requirements," which are time-sensitive and are expressed directly to NSA by the requesting agency. NSA exercises discretion in responding to these requirements; it also accepts requests from the executive branch agencies. NSA does not generate its own requirements.

All requirements levied on NSA must be for foreign intelligence. Yet, the precise definition of foreign intelligence is unclear. NSA limits its collection of intelligence to foreign communications and confines its activities to communications links having at least one foreign terminal. Nevertheless, this is based upon an internal regulation and is not supported by law or executive branch directive.

Although NSA limits itself to collecting communications with at least one foreign terminal, it may still pick up communications between two Americans when international communications are involved. Whenever NSA chooses particular circuits or "links" known to carry foreign communications necessary for the production of foreign intelligence, it collects all transmissions that go over those circuits. Given current technology, the only way for NSA to prevent the processing of communications of U.S. citizens would be to control the selection, analysis, or dissemination phases of the process.

Communications intelligence has been an integral element of United States intelligence activities. Foreign communications have been intercepted, analyzed, and decoded by the United States since the Revolutionary War. During the 1930s, elements of the Army and Navy collected and processed foreign intelligence from radio transmissions. Much of their work involved decryption, as well as enciphering United States transmissions. Throughout World War II, their work contributed greatly to the national war effort.

Since President Truman authorized NSA's establishment in 1952 to coordinate United States cryptologic and communications activities, tremendous advances have been made in the technology of communications intelligence. These advances have contributed to an expansion in demands for a wider variety of foreign intelligence and of requirements placed upon NSA/CSS SIGINT personnel and resources. As new priorities arise in the requirements process, greater demands will be placed upon NSA.

It is also necessary to face the problem of integrating intelligence requirements for foreign policy and national security with Constitutional constraints and safeguarding of domestic civil liberties. NSA's intercept programs and possible violation of Fourth Amendment rights are discussed in the section, "National Security Agency Surveillance Affecting Americans," in the Committee's Domestic Intelligence Report.

E. Military Counterintelligence and Investigative Activities

1. Background

The Department of Defense defines "military counterintelligence and investigative activity" as all investigative activity apart from foreign intelligence-gathering. Although this nomenclature is rela-

tively recent, the military services have always conducted investigations. None of these investigative activities are expressly authorized by statute; rather, they have been justified as necessary to the military mission. On occasion, investigative activity by the military has exceeded measures necessary to protect or support military operations.

In 1917, for example, Colonel Ralph Van Deman of the Army intelligence bureau recruited civilians in the Army Reserve and used volunteer investigators to report on "unpatriotic" conduct. Van Deman's men were soon dispersed throughout the country, infiltrating such organizations as the Industrial Workers of the World, mingling with enemy aliens in major cities, and reporting on all types of dissenters and radicals. Much of this civilian surveillance continued after World War I, particularly in the area of labor unrest. In the 1920s the Army had "War Plans White" to deal with anticipated uprisings of labor and radicals. In 1932 the Chief of Army Intelligence collected information on the "bonus marchers" arriving in Washington, D.C.

Similarly the activities of the Office of Naval Intelligence (ONI) have not always been restricted to military affairs. Traditionally, ONI has provided security for naval contractors, guarded ships, searched crews, detected illegal radio stations, and investigated naval personnel, enemy sympathizers, and civilians whose activities were "inimicable to the interests of the Navy."

Then, in the late 1960s during a period of considerable civil unrest in the United States, the three services—particularly the Army—were called upon to provide extensive information on the political activities of private individuals and organizations throughout the country.[36]

2. Areas of Investigation

DOD's counterintelligence and investigative activities are conducted for many purposes, both within the United States and abroad.[37]

a. Violations of the Uniform Code of Military Justice.—The UCMJ is a code of criminal laws which applies to all military personnel of the Department of Defense. The Secretary of each military department is responsible for enforcement of its provisions within his department. Investigations of UCMJ violations take place within the United States and in foreign locations where military personnel are stationed.

b. Security Clearances.—The Department of Defense conducts background investigations to determine whether to award security clearances to its military and civilian personnel or to the personnel of civilian contractors. These investigations are done both in the U.S. and abroad.

---

[36] For a detailed description of this and other improper military investigative activities, see the Select Committee's report entitled "Improper Surveillance of Private Citizens by the Military."

[37] Examples include investigations of security leaks, investigations in support of the Secret Service, investigations of theft at the facilities of Government contractors, and investigations—once military forces have been called in—to suppress domestic violence. None of these activities, however, *currently* represents a significant expenditure of investigative effort.

Military intelligence units also have certain counterintelligence functions to perform which relate to a unit's combat responsibilities.

c. Counterespionage.[38]—Under an agreement with the Federal Bureau of Investigation,[39] each of the military departments conducts counterespionage investigations on military and civilian members of their respective military departments, although all such operations are controlled by the FBI. In overseas jurisdictions where military commanders have control over occupying forces, the military departments are given more latitude to conduct counterespionage investigations, but these are coordinated with the Central Intelligence Agency.

Counterespionage investigations may be offensive or defensive in nature. Offensive investigations seek to obtain information on the purposes or activities of a hostile intelligence service. Defensive counterespionage investigations involve the identification of military personnel who are working for agents of a hostile intelligence service. Counterespionage operations are undertaken in both domestic and foreign settings.

d. Threats to DOD Personnel, Property, and Operations.—This type of investigation is distinguished from a counterespionage investigation because no hostile intelligence agency is involved. Rather, the "threat" typically arises from civilian groups and individuals whose activities might subvert, disrupt, or endanger the personnel, property, or operations of DOD. While "threat" information is normally obtained from local law enforcement authorities, the military has traditionally reserved the right to conduct its own investigations of such matters both in the U.S. and abroad.

In summary, one should remember that "military counterintelligence and investigative activity" is not a static category. It includes investigations undertaken for any reason apart from foreign intelligence collection. These range from investigations of lost property to investigations of fraud at servicemen's clubs. Moreover, the four general categories cited above expand and contract to meet changing military needs and demands from the Executive.

3. Supervisory Structure

The Secretary of Defense is ultimately responsible for all counterintelligence and investigative activity conducted by the Department of Defense. However, the Secretary has delegated management responsibility for this activity to the Assistant Secretary of Defense (Comptroller).[40] He, in turn, has delegated this responsibility to the Deputy Assistant Secretary of Defense (Comptroller), who was assigned responsibility for the Defense Investigative Program Office (DIPO).

DIPO apportions counterintelligence and investigative resources within the Department of Defense. The Office has budgetary control of funds allocated for these activities, and provides policy guidance. However, although DIPO stays informed of activities of the investigative agencies, it does not exercise formal operational control over them. In fact, no element at the OSD level exerts centralized opera-

[38] The counterespionage investigations of the Department of Defense are described in detail in a classified staff report of the Committee.

[39] The Delimitations Agreement of 1949. Each of the military departments has promulgated the agreement as a departmental regulation.

[40] DOD Directive 5118.3.

tional control over counterintelligence and investigative activities.[41] The one Defense Department agency engaged in such activity, the Defense Investigative Service (DIS), and the three military departments largely retain independent operational control of their own activities.

4. The Defense Investigative Service (DIS)

DIS is the only Defense agency established specifically to carry out counterintelligence and investigative activities.[42] Created in 1972, its chief function is performance of all security clearance investigations for civilian and military members of the Department of Defense as well as for all employees of Defense contractors. DIS also has been assigned responsibility for conducting "such other investigations as the Secretary of Defense may direct," thus making it a special investigative arm of the Secretary.[43]

DIS performs the special function of operating a computer index known as the Defense Central Index of Investigations (DCH). This is a computerized index which contains not only references to previous security clearance investigations, but also references to virtually every DOD investigation conducted in the past.[44] According to recent congressional testimony, the DCII now contains references to DOD files on approximately 15 million Americans.[45] DIS does not maintain the files, but indicates to requesters which DOD counterintelligence and investigative agency holds the file.

DIS has 280 offices across the United States, staffed by 2,620 military and civilian employees. DIS does not have personnel located overseas, but is responsible for security clearance investigations that may require tracking down leads overseas. Normally, an overseas element of one of the services would support DIS in such cases.

5. The Military Departments

In the Navy and Air Force, all counterintelligence and investigative activity, in both domestic and foreign contexts, is centralized in one element. In the Army, such activity is dispersed.

a. Navy.—All foreign and domestic counterintelligence and other investigative activity in the Navy is carried out by the Naval Investigative Service (NIS). The Director of NIS reports to the Director of Naval Intelligence, who has responsibility for foreign intelligence gathering by the Navy. He, in turn, reports to the Chief of Naval Operations. In 1975, 169 military and 744 civilian personnel[46] were assigned to NIS.

---

[41] The Defense Intelligence Agency made an unsuccessful effort to gain control of these activities in the late 1960s.

[42] The National Security Agency and Defense Intelligence Agency also have small elements with counterintelligence and investigative functions. These elements exist solely to protect the activities of the agencies of which they are a part.

[43] DOD Directive 5105.42.

[44] The DCII is routinely purged of references to files which have been destroyed because of their age, files on deceased subjects, or files which DOD directives have stipulated may not be retained.

[45] Testimony of David O. Cooke, Deputy Assistant Secretary of Defense (Comptroller), House Subcommittee on Government Operations, 1975 (unpublished).

[46] NIS agents are all civilian employees.

b. Air Force.—All Air Force investigative activity is carried out by the Air Force Office of Special Investigations (AFOSI). In contrast to NIS, the Director of AFOSI reports to the Air Force Inspector General. In 1975, AFOSI had 1,537 military and 384 civilian personnel assigned to it.

c. Army.—In the Army, criminal investigations are separated from other types of counterintelligence and investigative activity. They are carried out worldwide by the United States Army Criminal Investigation Command, the Director of which reports directly to the Army Chief of Staff.

Remaining counterintelligence and investigative activities are apportioned between the United States Army Intelligence Agency (USAINTA) and the military intelligence units located overseas. USAINTA has responsibility for all activities within the United States and in overseas locations where military intelligence units are not located. Where military intelligence units are part of Army forces stationed overseas (e.g., West Germany and Korea), they ordinarily carry out counterintelligence and investigative activity in their respective locations. Where an investigation proves to be beyond their capacity, USAINTA elements may be called upon.

Both the commanding office of USAINTA and the commanders of military intelligence groups overseas report to the Army Assistant Chief of Staff for Intelligence, who is responsible for the foreign intelligence-gathering activities of the Army. In 1975, the Army had assigned 2,822 military and 1,346 civilian personnel to counterintelligence and other investigative activities.

6. Results of Select Committee Inquiry

The Select Committee carried out an extensive investigation of the counterintelligence and investigative activities of DOD insofar as they have resulted in illegal and unwarranted intrusions into the political affairs of civilians. The results of the investigation are published in detail in the Committee Report entitled "Improper Surveillance of Private Citizens by the Military."

The Committee found that while certain of DOD's past counterintelligence and investigative functions resulted in the collection of information on the political activities of private citizens, DOD has effectively brought its counterintelligence and investigative activities under control since 1971. The Committee found that DOD currently maintains little information on unaffiliated individuals; that which it does maintain arguably falls within the terms of the Department's internal restrictions. Similarly, the Committee found that operations against civilians had been authorized in accordance with departmental directives.

Despite the success of the Department's internal directives to limit intrusions into the civilian community, the Committee nevertheless finds them inadequate protection for the future and recommends that more stringent legislative controls be enacted.

F. Chemical and Biological Activities

The terrible wounds inflicted by chemical weapons, such as chlorine and mustard gas, in World War I spawned international attempts to ban their use in warfare. The 1925 Geneva Convention succeeded

only in banning first use in war of chemical and biological weapons. The United States signed this Convention but Congress failed to ratify it; thus, the United States was not bound by its prohibitions. Nevertheless, there was a widespread belief that the United States would comply with the Convention.

Since the ban applied only to a country's first use of these agents, both the Allied and the Axis powers in World War II researched and stockpiled chemical and biological weapons in order to retaliate against first use by an enemy. Ironically, as the first President publicly to commit the United States to the policy of the Geneva Convention, President Roosevelt announced in June 1943, with the intent of warning Japan against the use of such weapons: "I state categorically that we shall under no circumstances resort to the use of such weapons [poisons or noxious gases] unless they are first used by our enemies." As he spoke, however, he knew the United States had intensified its biological research effort three months earlier with the construction of a facility for drug research at Fort Detrick, Maryland.

The threat of retaliation against a country using such weapons was effective. Although Germany was thought to have a stockpile, it did not touch it, even in the last desperate months of World War II. After the War, the United States program of research and development on such agents continued in order to maintain a weapons capability sufficient to deter first use by hostile powers. The Army's facility at Fort Detrick remained the center of biological weapons research and development.

1. Chemical and Biological Activities [46a]

Against this background, the Central Intelligence Agency entered into a special agreement with the Army on a project which the CIA codenamed MKNAOMI. The original purpose of MKNAOMI is difficult to determine. Few written records were prepared during its 18-year existence; most of the documents relating to it have been destroyed; and persons with knowledge of its early years have either died or have been unable to recall much about their association with the project. However, it is fair to conclude from the types of weapons developed for the CIA, and from the extreme security associated with MKNAOMI, that the possibility of first use of biological weapons by the CIA was contemplated.

The Army agreed that the Special Operations Division (SOD) at Fort Detrick would assist the CIA in developing, testing, and maintaining biological agents and delivery systems. By this agreement, CIA acquired the knowledge, skill, and facilities of the Army to develop biological weapons suited for CIA use. In 1967, the CIA summarized MKNAOMI objectives:

> a. To provide for a covert support base to meet clandestine operational requirements.
>
> b. To stockpile severely incapacitating and lethal materials for the specific use of TSD [Technical Services Division].
>
> c. To maintain in operational readiness special and unique items for the dissemination of biological and chemical materials.

[46a] See Chapter XVI.

d. To provide for the required surveillance, testing, upgrading, and evaluation of materials and items in order to assure absence of defects and complete predictability of results to be expected under operational conditions.[47]

In reviewing the records and testimony of SOD personnel, it is easy, for the most part, to distinguish SOD's work for the Army from its work for the CIA, even though very few SOD scientists knew of the CIA connection. For example, the CIA personnel who worked with SOD were identified as military officers from the fictitious Staff Support Group, whose interest in SOD was markedly different from the Army's. The CIA was careful to ensure that its moneys were transferred to SOD to cover the cost of CIA projects and the few existing SOD records indicate which projects were to be charged against the funds received from "P-600," the accounting designation for CIA funds.

SOD's work for the Army from 1952 until the early 1960s was primarily to assess the vulnerability of sensitive installations, such as the Pentagon, air bases, and subway systems, to biological sabotage by an enemy. In order to conduct these tests, SOD personnel would develop small, easily disguised devices—such as spray cannisters and spray pens—containing harmless biological agents. SOD personnel would surreptitiously gain access to the installation, leaving the devices to release the biological agent. SOD personnel would then monitor its spread throughout the installation. In this way, SOD could determine how vulnerable the installation was to sabotage of this kind and could advise those charged with security of the installation on countermeasures.

Although the CIA was interested in the kinds of delivery devices which SOD could make for delivery of the biological agents, CIA projects were distinct because they involved the mating of delivery systems to lethal or incapacitating biological agents, instead of harmless agents used in vulnerability tests. The CIA would ask SOD to produce a delivery system and a compatible biological agent—a request not made by the Army until the early 1960s.

SOD developed pills containing several different biological agents which could remain potent for weeks or months, and dart guns and darts coated with biological agents. SOD also developed a special gun for firing darts coated with a chemical that could incapacitate a guard dog in order to allow CIA agents to knock out the guard dog silently, enter an installation, and return the dog to consciousness when leaving. SOD scientists were unable to develop a similar incapacitant for humans.

SOD on occasion physically transferred biological agents in "bulk" form, various delivery devices, and most importantly, delivery devices containing biological agents, to CIA personnel. Although none of the witnesses before the Select Committee could recall any transfer of such materials for actual use by the CIA, evidence available to the Committee indicates that the CIA attempted to use the material. It is fair to conclude that biological agents and delivery devices prepared at Fort Detrick and transferred to the Staff Support Group were carried

[47] Memorandum from Chief, TSD/Biological Branch to Chief, TSD, "MKNAOMI: Funding, Objectives, and Accomplishments," 10/18/67, p. 1.

by CIA agents in attempted assassinations of foreign leaders. However, the Committee found no evidence that such material was ever in fact used against a person by the CIA.

By the early 1960s, the Army also became interested in the type of work SOD was doing for the CIA. The Army apparently decided that this type of surreptitious delivery device might be useful to Special Forces units in guerrilla warfare. SOD developed special bullets containing poison darts which could be fired, with little noise, from standard military weapons and small portable devices capable of spraying biological agents into the air which would form lethal clouds. Ultimately, the Army stockpiled a quantity of these bullets, but never transferred them to field units.

SOD developed another capability according to existing records which, so far as the Committee could determine, was never tapped by Army or by the CIA. Whereas most SOD work was devoted to biological weapons which would kill one individual noiselessly and with almost no trace of which would kill or incapacitate a small group. SOD did research the possibilities of large-scale covert use of biological weapons. SOD scientists prepared memoranda, which were passed to the CIA, detailing what diseases were common in what areas of the world so that covert use of biological weapons containing these diseases could easily go undetected. SOD researched special delivery devices for these biological agents, but it never mated such delivery devices with biological agents.

In addition to CIA interest in biological weapons for use against humans, it also asked SOD to study use of biological agents against crops and animals. In its 1967 memorandum, the CIA stated:

> Three methods and systems for carrying out a covert attack against crops and causing severe crop loss have been developed and evaluated under field conditions. This was accomplished in anticipation of a requirement which was later developed but was subsequently scrubbed just prior to putting into action.

2. Termination

All the biological work ended in 1969. Shortly after taking office, President Nixon ordered the staff of the National Security Council to review the chemical and biological weapons program of the United States. On November 25, 1969, he stated that the United States renounced the use of any form of biological weapons that kill or incapacitate. He further ordered the disposal of existing stocks of bacteriological weapons.

On February 14, 1970, the President clarified the extent of his earlier order and indicated that toxins—chemicals that are not living organisms but are produced by living organisms—were considered biological weapons subject to his previous directive. The Defense Department duly carried out the Presidential directive according to the instructions and supervision of the National Security Council staff. However, a CIA scientist acquired from SOD personnel at Fort Detrick approximately 11 grams of shellfish toxin, a quantity which was approximately one-third of the total world production and which was sufficient to prepare tens of thousands of darts. This toxin, a known danger

if inhaled, swallowed, or injected, was then stored in a little-used laboratory at the CIA where its presence went undetected for five years.

The transfer from SOD to the CIA resulted in a major quantity of the toxin being retained by an agency in a manner which clearly violated the President's order. The evidence to the Committee established that the decision to transfer and to retain the shellfish toxin was not made by, or known to, high-level officials of either the Defense Department or the CIA. The Director of the CIA was told of the possibility of retaining the toxin, but he rejected that course of action. The Committee found that the decision to keep the toxin, in direct and unmistakable contradiction of a widely announced Presidential decision, was made by a few individuals in the CIA and SOD.

Nevertheless, the history of MKNAOMI and the atmosphere surrounding it undoubtedly contributed to the mistaken belief of these individuals that they were not directly affected by the President's decision. The MKNAOMI project itself was contrary to United States policy since 1925 and to Presidential announcement since 1943, for it contemplated a first use of biological weapons by the CIA—albeit in the context of small covert operations. Moreover, because of the sensitive nature of MKNAOMI, these scientists gave their superiors little written record of their work and received little or no written guidance. The National Security Council staff, charged by the President with determining what U.S. policy should be, did not discover MKNAOMI in the course of its study and did not, therefore, consider the possibility that the CIA had biological weapons or biological agents. The CIA employee who claims to have made the decision, on his own, to retain the toxin received no written instructions to destroy them. Kept outside the National Security Council's study, the employee had to rely only on the newspaper account of the President's announcement and on his own interpretation of it.

G. Meeting Future Needs in Defense Intelligence

The defense intelligence establishment poses two fundamental problems for future national policy. The first is how to improve the quality of intelligence and ensure that intelligence collection and production are responsive to the needs of both the executive and legislative branches; the second is how Congress can exercise responsible oversight of the intelligence agencies. These goals require not only executive-legislative cooperation in control of the intelligence establishment, but also the design of a managerial and consultative system which is conducive to efficiency in routine activities, and adaptive to new priorities.

1. Anticipating New Requirements

It is a truism that generals should not plan for the next war by preparing for the last one; so too the intelligence community should not simply prepare to predict the last crisis. Ideally, allocation of intelligence resources should *precede* crises, not follow them. For example, concentration of a larger proportion of intelligence assets on economic issues should have begun before the 1973 oil embargo and energy crisis, not subsequently. In order to anticipate threats, which is the essential function of peacetime defense intelligence, the agencies

must strengthen their ability to anticipate the proper targets for collection and analysis.

The fundamental task of military intelligence will always be to detect the numbers, characteristics, and locations of enemy weapons, personnel, communications, and intelligence systems. As the world changes, however, the identities of enemies and the relative importance of different security threats change. The allocation of intelligence resources which was appropriate in a bipolar world, where the most likely threats were strategic nuclear war or large-scale conventional military engagements in the third world, is less appropriate in a world where power is becoming more diffused. For example, although the energy crisis (which is increasing the spread of nuclear power reactors and eroding the technical and economic barriers to acquiring nuclear weapons) and the growth of regional power rivalries (which increases incentives to acquire such weapons) are combining to make nuclear proliferation an imminent threat, the Air Force unit responsible for nuclear intelligence still directs virtually all of its assigned technical collection resources against the USSR and China.[48]

In the short range, it is obvious that problems such as nuclear proliferation and international terrorism will be given increasingly high priorities in national intelligence. Since DOD has the vast majority of collection assets, it should be increasingly involved in these problem areas. In doing so, a new balance may have to be struck between the national/peacetime intelligence priorities of the Department of Defense and the intelligence community as a whole, and the tactical/wartime requirements of the military. The critical problem for improving intelligence in the long-range, however, is to identify the mechanisms which are conducive to adaptation, re-evaluation of priorities, and flexible distribution of collection and analysis assets. Feedback from consumers of national intelligence—such policy and research agencies as ISA, DDR&E, State, NSC, ERDA, and ACDA—should be regularized, and DOD should also be responsive to the community-wide committees (such as IRAC, NSCIC, USIB, or IC Staff) which consider the interface between issue urgency and collection capabilities.

2. Effects of New Technology

Technological change produces both new capabilities and new barriers in intelligence collection. Unless the U.S. loses its wide lead in capacity for technological innovation, however, scientific advances are likely to be a net benefit.[48a]

In the near future, expanded computer capabilities can be expected to improve the integration and availability of processed information by use of a central bank with data, pictures, and reports digitized for quick retrievability according to title or substance. This would offer the efficiency and thoroughness of a full text search, but it also raises the issue of the proper extent of compartmentation.

Improved technology also offers hedges against vulnerability and political sensitivity. Development of unmanned mobile sensors for dangerous peripheral reconnaissance missions can eliminate most of the risks in current collection programs, or the potential for crises

[48] Air Force briefing for Select Committee staff, July 1975.
[48a] See the Committee's detailed report on Intelligence and Technology.

and embarrassments which followed the North Korean seizure of the *Pueblo* and downing of the EC–121. Both a reduction in risk and an increase in cost-effectiveness could be possible if improved technology results in substantial manpower reductions.

Technology is interactive. Availability of new techniques for monitoring or verification may provoke enemy countermeasures, and enemy development of new weapons systems can produce the need for new techniques of verification. (Heavy deployment of cruise missiles or development of mobile land-based ICBMs by either the U.S. or U.S.S.R., given current detection capabilities, would create virtually insoluble problems of verification of strategic arms limitation agreements. Development by either side of certain technical innovations, on the other hand, could be undesirable. A breakthrough in ability to detect and fix the location of submarines, for example, would destabilize mutual nuclear deterrence by increasing the vulnerability of the other side's second-strike capability.) The complex dynamics of these interactions require substantial attention to coordinating R&D for intelligence with policy considerations. The expense which goes with technical sophistication also suggests the need for rigorous cost-benefit analysis in intelligence R&D, to judge the relative utility of new capabilities.

3. Restructuring Defense Intelligence Organizations

The pattern of DOD intelligence organization is obviously important for the division of authority and responsibility within the departments, but it also has ramifications for the control and direction of the intelligence community as a whole. Internally, there are divergent interests and needs, particularly between the civilian leadership in OSD and the military leadership in the JCS and unified commands. Externally, there is an imbalance between the responsibility of the DCI to direct the collection and production of national intelligence, and the predominance of DOD in control of actual assets.

Within the defense establishment there has traditionally been a trade-off in the view of many observers, between the peacetime needs of the Secretary of Defense for "national" intelligence on general politico-military developments and trends, and the wartime needs of the professional military for "tactical" intelligence on enemy forces and operations. This distinction may be eroding since central national sensors can have important tactical applications.

Nevertheless, the Secretary of Defense and JCS have different responsibilities, and thus different intelligence priorities. Dissatisfaction with fragmentation and duplication of service intelligence support to the Secretary led to the formation of the Defense Intelligence Agency 15 years ago. The DIA was supposed to integrate military intelligence activities, and to serve the needs of both OSD and the services. There has been widespread criticism of DIA's performance since it was created.

The new Deputy Secretary of Defense position is designed to assert greater control of DOD intelligence from the OSD level. If OSD staff resources for intelligence are increased, and DIA's role is decreased, the trade-off between service needs and the needs of national leadership may be recognized, accepted, and dealt with, in contrast to the earlier attempt to "cure" the problem by combining managerial func-

tions in DIA. There has been a similar potential problem in NSA, although it has provoked far less concern than DIA since NSA must also serve national and tactical needs. In 1961 the JCS attempted to gain control of that agency,[49] and in recent years some critics at the other extreme have suggested taking NSA out of DOD, since it serves many non-military needs. The entire problem of dealing with the mutual relations of national and tactical intelligence may be clarified as the DCI assumes the additional authority granted to him by the President's Executive Order of February 18, 1976.

While establishment of a Pentagon intelligence czar in the form of the new Deputy Secretary may reduce fragmentation within the department and improve the coherence of military intelligence, it will probably have a major impact on the coordinating role of the DCI. Given that the overwhelming volume of total U.S. intelligence collection and production occurs within DOD, the Deputy Secretary could become, in effect, a second DCI. The definition of the relation between these two officials will be the single most critical factor in top-level organization for management of national intelligence.

4. Requirements for Congressional Oversight

If Congress attempts to exercise more comprehensive and detailed oversight of intelligence agencies, the biggest issue is likely to be what information the executive branch should make available. On defense intelligence there is likely to be less of a problem if Congress concentrates on issues of intelligence process rather than substance. There is, of course, a limit as to how far it is possible to evaluate the former without considering the latter. Therefore, norms will have to be established about what kinds of material (for example, finished intelligence) will be subject to scrutiny by Congress on a routine basis. Provision should also be made to keep basic information on budgets and resource allocation in a clear and available form in the Pentagon, obtainable by the oversight committee on demand. More consistent and thorough documentation of the chain of command could also be required in internal correspondence (thus avoiding the problem of "unattributable" records of controversial decisions turning up in the files, i.e., unsigned directives or cables which cannot clearly be traced to an authoritative source).

If independent ongoing oversight of the substance of defense intelligence is the goal, an oversight committee should have staff expertise in several areas: (1) Political, to weigh the risks and gains of certain programs and targets; (2) Scientific and Technical, to evaluate sensors; (3) Economic, to judge cost-effectiveness; (4) Military, to consider non-national strategic and tactical requirements of DOD intelligence.

---

[49] Memorandum from the Chairman of the Joint Chiefs of Staff Lemnitzer to Secretary of Defense McNamara, 3/2/61.