

CHAPTER 18

INTELLIGENCE

"We exist to support a transforming Army by fielding and sustaining the world's premier Military Intelligence Organization."

Lieutenant General Robert W. Noonan, Jr., Deputy Chief of Staff for Intelligence, Headquarters, Department of the Army

SECTION I INTRODUCTION

18-1. Chapter content

a. Army Military Intelligence provides commanders, operators, and other consumers timely and accurate information and finished intelligence for the commander to identify the enemy's center of gravity and to conduct dominate operations at every echelon. Intelligence is also an integrated element of battle command and a fundamental enabler for information operations (IO).

b. This chapter defines intelligence and provides an overview of the need for intelligence by decision makers. It includes the composition and responsibilities of the various intelligence organizations at national, Department of Defense (DOD), non-DOD, and Service (including HQDA) levels. It also describes the Army concepts for the production of intelligence and the relationship of intelligence to operations security; targeting; electronic warfare; and the requirement for seamless intelligence support "from space to mud".

c. Intelligence is the product obtained from the systematic planning and directing, collection, processing, analysis and production, and dissemination of information. This chapter addresses the management of this effort.

18-2. Intelligence drivers

a. Presidential direction. President Reagan signed Executive Order (EO) 12333 on 4 December 1981. The EO provides for the effective conduct of U.S. intelligence activities and the protection of the constitutional rights of U.S. citizens. EO 12333 superseded EO 12036, which regulated U.S. intelligence activities during the Carter Administration. The original EO on the subject was 11905, signed by President Ford. EO 12333 has not been superseded under subsequent administrations. The Army implements EO 12333 through Army Regulations 381.10 and 381-20. President Clinton signed a Presidential Decision Directive (PDD) entitled U.S. Counterintelligence Effectiveness – Counterintelligence for the 21st Century on 5 January 2001. The PDD directed the establishment of a National Counterintelligence Board of Directors chaired by the Director, Federal Bureau of Investigations (FBI) and composed of the Deputy Secretary of Defense, Deputy Director of Central Intelligence (DDCI) and a senior representative of the Department of Justice. It also directed the establishment of a National Counterintelligence

Executive to serve as the substantive leader of national-level counterintelligence and execute responsibilities on behalf of the National Counterintelligence Board of Directors. In addition, the PDD outlines other specific steps that will enable the U.S. counterintelligence community to better fulfill its mission of identifying, understanding, prioritizing and counteracting the intelligence threats faced by the United States.

b. Army Transformation. Military Intelligence (MI) is an integral element of the Army's Transformation goals and objectives. The Army is developing a single, cohesive picture of Army MI in the future, that is who and what Army MI must be, and what direction Army MI must take to support the commander during full spectrum operations. This foundation builds from a vision and guiding set of principles for MI: quality people and leadership; focused analysis and synthesis; integrated in facilitating situational understanding; gaining information superiority; support to force protection; and the ability to leverage joint and national intelligence support. Each principle provides overarching guidance and direction Army MI soldiers and civilians need to accomplish MI's mission.

(1) As the Army transitions to provide rapid, decisive, and sustained land power, MI requires a new approach toward conducting intelligence operations. Intelligence sources currently collect, process, analyze, and disseminate information as either single or multidiscipline intelligence, focused principally on collection methods and capabilities. Within this architectural framework, the ability to rapidly share critical, time-sensitive information is hindered. The commanders' need for a shared, up-to-the minute understanding of the battlespace, coupled with the explosion of the availability of information, mandates a shift toward creating a collaborative, distributed, and integrated information environment as illustrated in Figure 18-1.

(2) Implementing this vision will require the Army to integrate intelligence, surveillance, and reconnaissance to help shape the battlespace from the strategic to the tactical levels; to leverage national agencies and sister services to better support the warfighter; and focus on core intelligence competencies. Changes in Army intelligence that support this vision include the use of intelligence support elements at all levels and changes to the intelligence force structure that better support a strategically deployable Army.

c. Need for intelligence. Timely, relevant, accurate, predictive and useable intelligence addressing the activities, capabilities, plans, and intentions of foreign leaders and their governments is needed to develop sound national security and foreign policies. It is critical to international negotiations and to the development and monitoring of international agreements.

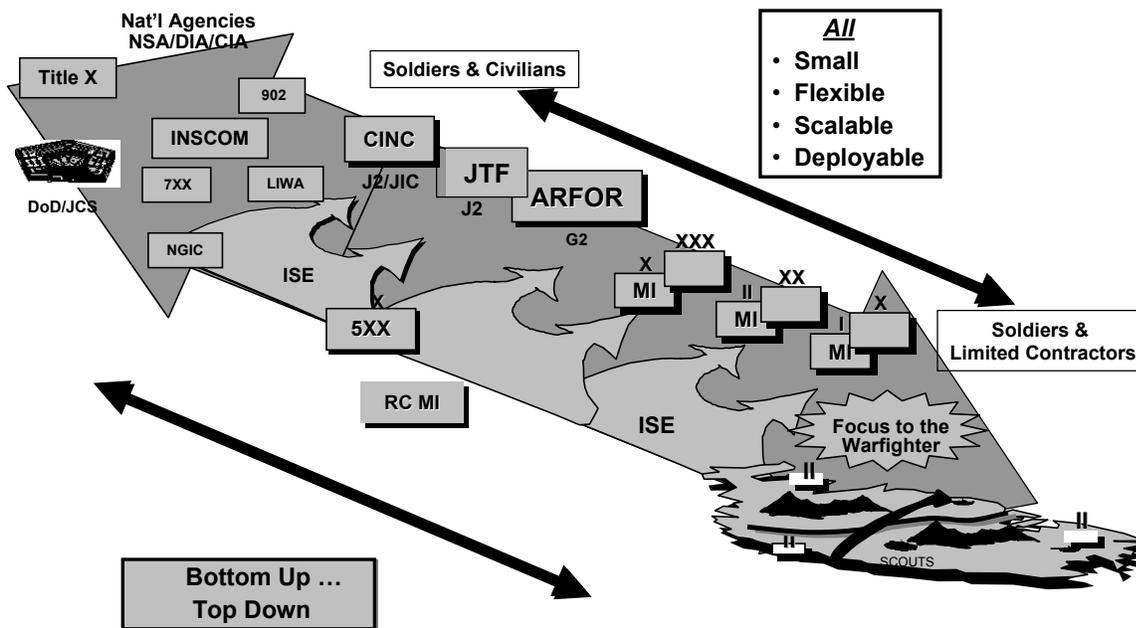


Figure 18-1. Army Intelligence—Changing Methods and Balance

(1) Within the DOD, planners and managers responsible for the development of weapons systems and force structure need accurate, long-range projections of the combat capabilities and technologies of foreign powers as the basis for their recommendations and decisions. The ability of U.S. forces to deter or defend against attack requires detailed knowledge of the current deployment and capabilities of potential adversaries and their future plans.

(2) At the operational and tactical levels of warfare, intelligence must provide a commander with information and knowledge in order to facilitate situational understanding so that he or she can position and employ his or her forces successfully to accomplish the assigned mission. It is a key component of battle command and will provide the enemy and environment portions of the common operating picture to the commander and his or her staff. Finally, as our focus shifts to strategic responsiveness, the potential for a rapid deployment into a small scale contingency requires detailed information on the cultural, historical, economical, technological, and political factors of the area in which they will deploy. One technique to meet this requirement is a new concept termed intelligence reach. The amount and fidelity of intelligence necessary to maintain strategic responsiveness and to counter asymmetric threats require a tremendous amount of information to ensure mission accomplishment with minimal casualties and limited collateral damage.

18-3. Intelligence products

a. Categories of intelligence. Intelligence products may be categorized in several ways depending on the needs of the intended recipients as well as the scope, level of detail, and the perishability of the product. The distinctions between these types of intelligence products are becoming less pronounced as the nature of offensive, defensive, stability, and support operations overlap within any larger operation. Additionally, technology, including web-enabled technology, facilitates the development, acquisition, and integration of all-source intelligence through a “seamless” architecture from the national to the tactical levels. Examples include the U.S. Army’s All Source Analysis System (ASAS), the Joint Worldwide Intelligence

Communications System (JWICS), the Joint Deployable Intelligence Support System (JDISS), and other similar types of multidimensional systems and capabilities.

(1) National intelligence is integrated departmental intelligence coordinated by the National Foreign Intelligence Board (NFIB) and approved by the Director of Central Intelligence (DCI). It covers the broad aspects of national policy and national security, is of concern to more than one department or agency, and transcends the exclusive competence of a single department or agency.

(2) Departmental intelligence is intelligence that any department or agency of the Federal Government requires to execute its own mission. This may include any or all of the following: National Security Council (NSC) Staff, Central Intelligence Agency (CIA), Department of State and its intelligence and research (INR) staff, Department of the Treasury (Secret Service and the Bureau of Alcohol, Tobacco, and Firearms), Department of Justice (FBI), Department of Transportation (U.S. Coast Guard); the National Drug Enforcement Office; and the DOD and its agencies to include the Defense Intelligence Agency (DIA), National Security Agency (NSA), National Imagery and Mapping Agency (NIMA), National Reconnaissance Office (NRO), and the Armed Forces.

b. Levels of intelligence.

(1) Strategic intelligence is intelligence required for the formulation of strategy, policy, and military plans and operations at theater level and above. Strategic intelligence—

- Concentrates on the national political, economic, and military considerations of a state
- Identifies a nation's ability to support U.S. Forces and operations (for example, ports and transportation infrastructure)
- Predicts other nation's responses to U.S. operations.

(2) Operational intelligence is the intelligence required for planning and conducting campaigns and major operations to accomplish strategic objectives within theaters or areas of operations. Intelligence at this level serves as a bridge between strategic and tactical levels. Operational intelligence—

- Supports friendly campaigns and operations by predicting the enemy's campaign plans, identifying their military centers of gravity, lines of communication, decisive points, pivots of maneuver, and other components necessary for campaign design.
- Focuses primarily on the intelligence needs of commanders from theater through corps and task force.

(3) Tactical intelligence is intelligence required for planning and conducting tactical operations as an integral part of battle command. Intelligence provides the tactical commander with the information and knowledge that is needed to reach situational understanding and employ allocated forces in order to meet assigned objectives. Tactical intelligence is distinguished from other levels by its perishability and ability to quickly influence the outcome of the commander's mission.

c. Types of intelligence.

(1) Basic intelligence is encyclopedic type information, which is not time-sensitive and describes all aspects of a nation - physical, social, economic, political, geographical, cultural, and military - which is used as a base for intelligence products in support of planning, policymaking, and military operations.

(2) Current intelligence includes all types and forms of perishable, time-sensitive, information of immediate value and interest to specific consumers. It may be disseminated without complete evaluation, interpretation, analyses, or integration.

(3) Estimative intelligence is that intelligence which projects forward in time and is predictive in nature.

(4) Crisis intelligence is comprised of specific types and forms of very perishable, time-sensitive information of immediate value, and usually intense interest at the international, national, and theater levels. It is narrowly focused on a precise area, individual(s), or event, which is closely monitored until termination or closure. Usually after 30 days, this type of intelligence becomes current intelligence and eventually basic intelligence.

(5) Combat information is data obtained through intelligence collection sources and methods, which are passed rapidly to the user without benefit of analysis, interpretation, or integration. A sensor-to-shooter system transmitting highly perishable, potential targeting data, is an example of this data. Tactical commanders often must make decisions based on the immediate access to and availability of combat information.

d. Intelligence disciplines.

(1) Intelligence is categorized by a series of interdependent disciplines. No single discipline can normally satisfy the commander's requirements. The actual mix of disciplines tasked to satisfy a requirement is situation dependent.

(2) Human intelligence (HUMINT) is a category of intelligence derived from information collected and provided by human sources as opposed to technical sources. HUMINT includes such overt activities as attaché duty, liaison functions, interrogation of prisoners of war, debriefing of displaced persons/refugees/evacuees/and line crossers, solicitation of information from indigenous persons, document exploitation, and controlled collection operations such as clandestine operations. A HUMINT collector is a person, who by training is tasked with and engages in the collection of information from individuals for the purpose of answering specific intelligence requirements.

(3) Imagery intelligence (IMINT) is intelligence derived from the exploitation of collection by visual photography, infrared sensors, lasers, electro-optics, and radar sensors such as synthetic aperture radar wherein images of objects are reproduced optically or electronically on film, electronic display devices, or other media. The resulting imagery may be analyzed in either hard-copy (photographic) or soft-copy (electronic display) format for distribution.

(4) Signals intelligence (SIGINT) is intelligence obtained through the exploitation and analysis of electromagnetic emissions and includes communications intelligence, electronic intelligence, and foreign instrumentation SIGINT.

(5) Measurement and signature intelligence (MASINT) uses information collected by technical means such as radars, lasers, passive electro-optical sensors, radiation detector, seismic, and other sensors to measure objects or events to identify them by their signature. MASINT exploits other information that is not collected through SIGINT, IMINT, or HUMINT. It plays a significant role in theater missile defense. It includes unmanned aerial vehicle video and JSTARS moving target indicators.

(6) Technical intelligence (TECHINT) is a multidiscipline function that supports commanders by either identifying or countering an enemy's momentary technological advantage, or by maintaining a technological advantage. The two parts of TECHINT are battlefield

TECHINT and scientific and technical intelligence. TECHINT is also derived from the exploitation of foreign material produced for strategic, operational, and tactical commanders.

(7) Counterintelligence (CI) is that intelligence which deals with the information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, subversion, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or terrorist activities. CI is integrated with operations security (OPSEC) and force protection through the CI assessment of the vulnerability of specific U.S. Forces, areas, or activities to foreign intelligence collection, terrorist activities and other hostile operations by intelligence and security services.

(8) Open source intelligence (OSINT), within Army intelligence doctrine, is recognized as important information but OSINT is not recognized as a discipline. However, OSINT is a discipline within joint doctrine. Open source intelligence is intelligence derived from the collection and analysis of information, which is unclassified, and largely in the public domain. Open source intelligence may cut across other disciplines to include broadcast, imagery and mixed media sources. This type of information however must be carefully analyzed because it is potentially subject to inaccuracies and adversary deception.

SECTION II

THE NATIONAL FOREIGN INTELLIGENCE SYSTEM, SYSTEM MANAGEMENT AND OVERSIGHT, AND MANAGEMENT OF COLLECTION AND PRODUCTION

18-4. U. S. intelligence community goal and organization

The goal of the U.S. intelligence effort is to provide the President, the National Security Council, U.S. policymakers, and military leaders information on which to base decisions concerning the development and conduct of foreign, defense, and economic policy, and the protection of U.S. interests from foreign threats. To reach this goal, the U.S. intelligence community (IC) is organized as shown in Figure 18-2.

a. The National Security Council (NSC). The NSC supported by the NSC Staff reviews, guides, and directs the conduct of all national foreign intelligence, CI, special activities, and attendant policies and programs. Within the NSC system, the Senior Interagency Group - Intelligence formulates policy, monitors decisions, and evaluates the adequacy and effectiveness of collection efforts.

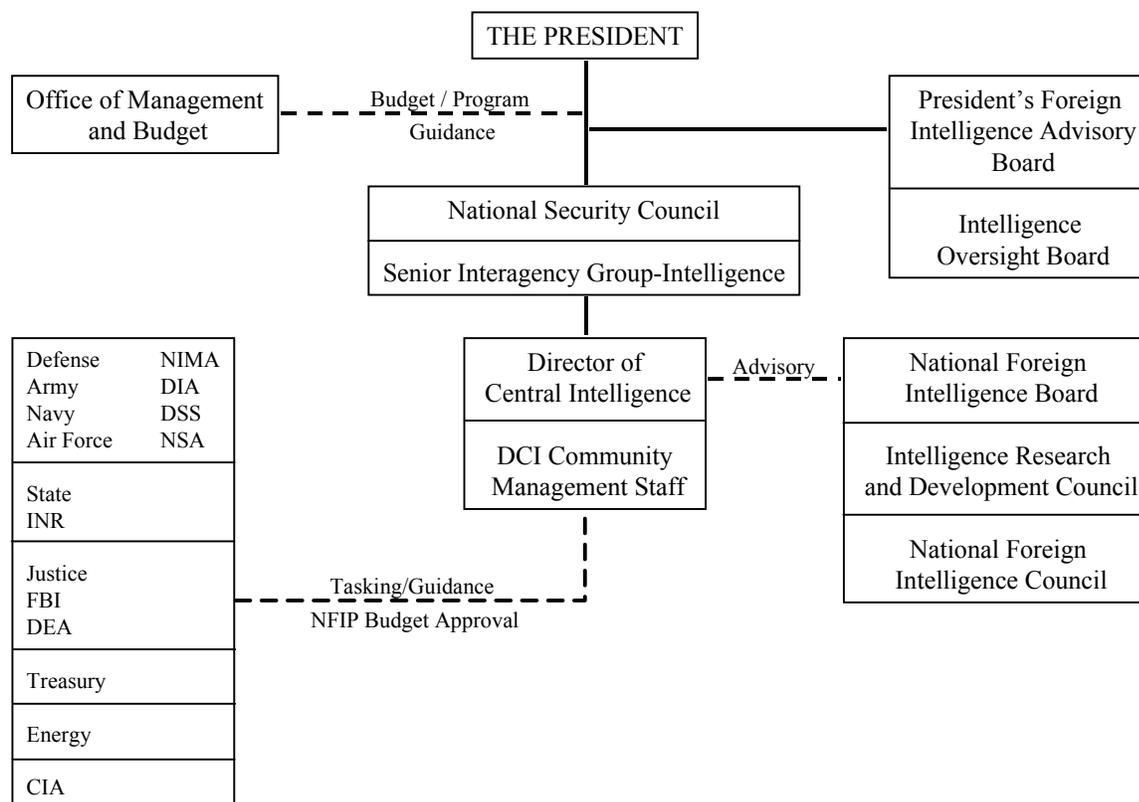


Figure 18-2. Organization of the National Intelligence System

b. The President's Foreign Intelligence Advisory Board (PFIAB).

(1) The PFIAB reports directly to the President and provides advice concerning the objectives, conduct, management and coordination of the various activities of the agencies of the IC. In addition to the President, the DCI, the CIA, or other government agencies engaged in intelligence activities can request PFIAB recommendations concerning ways to achieve increased effectiveness in meeting national intelligence needs.

(2) By Executive Order 12863, signed by President Clinton on 13 September 1993, the Intelligence Oversight Board (IOB) was established as a standing committee of the PFIAB. The IOB is required to report through the PFIAB to inform the President of intelligence activities that any member of the Board believes are in violation of the Constitution or laws of the United States, Executive orders, or Presidential directives; to forward to the Attorney General reports received concerning intelligence activities that the Board believes may be unlawful; to review the internal guidelines of each agency within the IC concerning the lawfulness of intelligence activities; to review the practices and procedures of the inspectors general and general counsels of the IC for discovering and reporting intelligence activities that may be unlawful or contrary to an Executive order or Presidential directive; and to conduct such investigations as the Board deems necessary to carry out its functions under this order.

c. The Director of Central Intelligence (DCI). The DCI is concurrently Director, CIA, and is directly responsible to the President and the National Security Council. The DCI is the primary adviser to the President and other members of the NSC on national foreign intelligence and is the intelligence system's principal spokesman to Congress. The DCI develops objectives and prepares guidance for the IC to enhance its capabilities for responding to expected future needs for foreign national intelligence, formulates policies concerning intelligence arrangements with foreign governments, and coordinates intelligence arrangements between agencies of the IC

and the intelligence or internal security services of foreign governments. The DCI is responsible for the development, presentation, and justification of the National Foreign Intelligence Program (NFIP) budget. A complete list of DCI responsibilities is contained in EO 12333.

(1) Other senior officials are responsible for contributing, within their areas of capability, to the national foreign intelligence collection effort and for cooperating with other IC members to achieve efficiency and provide mutual assistance. In addition, they are responsible for management of the collection of departmental intelligence.

(2) Pursuant to EO 12333, the DCI establishes boards, councils, committees, or groups as required for the purpose of obtaining advice from within the IC. Two of the advisory boards the DCI chairs are the National Foreign Intelligence Board and the Intelligence Community Executive Committee.

d. The Community Management Staff (CMS). The Community Management Staff was established by the DCI in 1992, replacing the Intelligence Community Staff. It is an independent element and its head is the Executive Director for Intelligence Community Affairs (EXDIR/ICA). The EXDIR/ICA is the DCI's principal adviser on IC matters and assists the DCI in planning and implementing national foreign intelligence production responsibilities. The CMS is charged with developing, coordinating, and executing the DCI's community responsibilities for resource management; program assessment and evaluation of policies; and collection requirements management. It also performs other functions and duties as determined by the DCI, Federal statutes, or executive action.

e. The National Intelligence Council (NIC). The NIC, managed by a chairman and a vice chairman, is comprised of National intelligence officers--senior experts drawn from all elements of the community and from outside the Government. The National intelligence officers concentrate on the substantive problems of particular geographic regions of the world and of particular functional areas such as economics and weapons proliferation. Through routine close contact with policymakers, collection, research, and community analysis, the NIC provides the DCI with the information needed to assist policymakers as they pursue shifting interests and foreign policy priorities. Finally the NIC assists the IC by evaluating the adequacy of intelligence support and works with the community's functional managers to refine strategies to meet the most crucial needs of our senior consumers.

f. National Foreign Intelligence Board (NFIB). The NFIB is responsible for approving all National intelligence estimates, for coordinating interagency intelligence exchanges and the numerous bilateral relationships with foreign nations that share intelligence with the United States, and for developing policy for the protection of intelligence sources and methods.

g. Intelligence Community Executive Committee (IC/EXCOM). The IC/EXCOM advises the DCI on priorities and objectives for the NFIP budget, national intelligence policy and planning, and IC management and evaluation. Permanent IC/EXCOM members include the DCI; DDCI; Vice Chairman, Joint Chiefs of Staff (VCJCS); Director, NSA; Director, DIA; Assistant Secretary of State and INR; Director, NRO; Director, NIMA; Chairman, NIC; Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD/C3I); and EXDIR/ICA.

h. Central Intelligence Agency (CIA). The Central Intelligence Agency is an independent agency, responsible to the President through the DCI, and accountable to the American people through the intelligence oversight committees of the Congress. The CIA's mission is to support the President, the NSC, and all officials who make and execute national security policy by: Providing accurate, comprehensive, and timely foreign intelligence on national security topics,

conducting CI activities, special activities, and other functions related to foreign intelligence and national security, as directed by the President.

(1) To accomplish this mission, the CIA works closely with the other organizations in the IC to ensure that the intelligence consumer—whether Washington policymaker or battlefield commander—receives the best intelligence possible. As a separate agency, the CIA serves as an independent source of analysis on topics of concern to these consumers.

(2) The CIA collects foreign intelligence information through a variety of clandestine and overt means. The Agency also engages in research, development, and deployment of high-leverage technology for intelligence purposes and - in support of the DCI's role as the President's principal intelligence advisor - performs and reports all-source analysis on the full range of topics that affect national security. The CIA is organized along functional lines to carry out these activities and to provide the flexible, responsive support necessary for its worldwide mission.

(3) Throughout its history, but especially as new global realities have reordered the national security agenda, the CIA has emphasized adaptability to meet the needs of intelligence consumers. To assure that all of the Agency's capabilities are brought to bear on those needs, the CIA has tailored its support for key policymakers and has established on-site presence in the major military commands.

(4) Also, the CIA contributes to the effectiveness of the overall IC by managing services of common concern in imagery analysis and open source collection, and by participating in strategic partnerships with other intelligence agencies in the areas of research and development and technical collection. Finally, the CIA takes an active part in community analytical efforts and coordinates its analytical production schedule with appropriate agencies to ensure efficient coverage of key topics.

(5) The Office of Military Affairs (OMA) was established in the CIA to support military plans and operations. The OMA falls under the Associate Director of Central Intelligence for Military Support, a flag rank military officer and provides a central point of contact to the military departments to facilitate coordination with the CIA.

18-5. Executive and Congressional intelligence resource management

The National Security Council provides overall executive branch guidance, direction, and review for all national foreign intelligence and CI activities. Within the legislative branch, the House Permanent Select Committee on Intelligence (HPSCI) and the Senate Select Committee on Intelligence (SSCI) along with the Foreign Relations, Foreign Affairs, and the Armed Services Committees are responsible for authorizing intelligence resources and overseeing intelligence activities. The appropriations committees are authorized by the Constitution to appropriate funds for all government activities, including intelligence activities. The NSC system has special committees within its framework, which deal with its intelligence responsibilities. In addition to the management of the individual agencies or elements thereof, which constitute the intelligence system, management of intelligence focuses mainly on intelligence resources, requirements, collection tasking, collection, analysis, production and dissemination. While not a member of the IC, the Office of Management and Budget provides program and budget guidance to the Director of Central Intelligence for development of the National Foreign Intelligence Program as part of the Federal budget. Within the DOD, the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) is the single DOD focal point for intelligence management

a. National Foreign Intelligence Program (NFIP). The NFIP provides funds for the bulk of all national-level intelligence, CI, and reconnaissance activities of the CIA, DOD, and all civilian Federal agencies and departments, as well as the IC management structure. The program is comprised of two major components – national level intelligence programs within the DOD and those in Federal departments and agencies outside DOD. The defense programs include the General Defense Intelligence Program (GDIP), the Consolidated Cryptologic Intelligence Program (CCP), the DOD Foreign Counterintelligence Program (FCIP), the National Imagery and Mapping Agency Program (NIMAP), the National Reconnaissance Program (NRP), and specialized DOD reconnaissance activities. The Program Manager for the GDIP is the Director, DIA; Program Manager for the CCP is the Director, NSA; Program Manager for the FCIP is the Director of Counterintelligence who is subordinate to the Deputy Assistant Secretary of Defense (Security and Information Operations), under the ASD(C3I). Program manager for the NIMAP is the Director, NIMA and program manager for the NRP is the Director, National Reconnaissance Office.

b. Joint Military Intelligence Program (JMIP). The JMIP focuses on joint, defense-wide initiatives, activities and programs that predominantly provide intelligence information and support to multiple defense consumers; bridge existing programmatic divisions across Service, departmental and national intelligence lines to provide more effective and coherent intelligence programmatic decision-making; and ultimately support military intelligence consumers, that is warfighters, policymakers, and force modernization planners. The JMIP is composed of four programs: the Defense Cryptologic Program, Defense Imagery and Mapping Program, the Defense Mapping, Charting and Geodesy Program and the Defense General Intelligence and Applications Program. The Defense General Intelligence and Applications Program, coordinated by the Director, DIA is further divided into five components. The components of this program include the Defense Airborne Reconnaissance Program, the Defense Intelligence Tactical Program, the Defense Intelligence Counterdrug Program, the Defense Intelligence Special Technologies Program, and the Defense Space Reconnaissance Program.

c. Combatant command and Service participation. Combatant commanders formally participate in the Capabilities Programming and Budgeting System and influence the DOD Planning, Programming, and Budgeting System (PPBS) process for intelligence resources through their Commander in Chief (CINC) Integrated Priority List. Through the Command Intelligence Architecture Program, combatant commanders identify their intelligence collection, processing, and dissemination resource requirements. The Command Intelligence Architecture Program has become the driving force for acquiring the requisite military intelligence capabilities into the 21st century.

(1) Within Headquarters, Department of the Army, the Deputy Chief of Staff for Intelligence (DCSINT) and DCSINT staff participate in the PPBS through the program evaluation groups and membership on the PPBS Council of Colonels, Planning, Programming, and Budget Committee, and Senior Resource Group.

(2) The Army participates directly in three of the programs of the National Foreign Intelligence Program: the Consolidated Cryptologic Program, the Foreign Counterintelligence Program and the General Defense Intelligence Program. Program and budget information is prepared by the Army and sister Services and forwarded through program managers to the DCI.

(3) In addition to the NFIP budget, many Army intelligence resources are included in the DOD Joint Military Intelligence Program and tactical intelligence and related activities (TIARA) funding. These programs include most intelligence resources directly supporting operational commanders at the joint and Service levels.

d. TIARA accounts. TIARA accounts provide funding for timely intelligence support primarily to tactical operations of military forces. TIARA activities and systems are planned, programmed, and executed by the military Services and U.S. Special Operations Command and compete for funding with the combat and combat-support programs they support. As defined by the Congress, TIARA funds represent those portions of the DOD budget devoted to Service level military intelligence activities outside the NFIP. TIARA is an aggregation of portions of the DOD budget that provide tactical intelligence and related support to military operations. In contrast to the NFIP, countless military officials on a decentralized basis manage TIARA assets.

e. Intelligence oversight. The Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence play key roles in the conduct of intelligence oversight. These roles, specified by law, require that the committees be kept fully and currently informed of all intelligence activities which are the responsibility of, are engaged in by, or are carried out for or on behalf of any department; that they be furnished any information or material concerning intelligence activities requested in order to carry out authorized responsibilities; and that the committees be informed in a timely fashion of any illegal intelligence activity or significant intelligence failure and any corrective action.

(1) Within the DOD the officer responsible for the oversight of intelligence activities is the Assistant to the Secretary of Defense for Intelligence Oversight (ATSD-IO). DOD Directive 5148.12, dated 20 July 1989, established the position and assigned its responsibilities. The ATSD-IO had been designated as the sole conduit between the DOD and the President's Intelligence Oversight Board. Upon the establishment of the JMIP, the Secretary of Defense (SecDef) also created the Defense Intelligence Executive Board as a management mechanism to provide oversight of Defense intelligence programs, and to make key decisions for the allocation of available resources to meet defense needs.

(2) The Army General Counsel and the Army Inspector General share responsibility for the oversight of intelligence activities within the Army.

18-6. Intelligence cycle

The intelligence cycle consists of planning and direction; collection; processing and exploitation; analysis and production; dissemination and integration; and evaluation and feedback. Intelligence collection and production management guide the bulk of the process and the expenditures of resources.

a. Collection management. The intelligence cycle begins and ends with the consumer. A consumer's requirements are passed to the producer for fulfillment. If the producer cannot satisfy the consumer's requirements, the producer levies the requirement on the collector. The user must be able to state clearly his or her intelligence interests or needs (requirements) in addition to those that are already satisfied by existing finished intelligence. Requirements compete for limited collection resources at the national, departmental, strategic, operational, and tactical levels. Requirements are prioritized in accordance with the intelligence requirements contained in a classified 2 March 1995 Presidential Decision Directive 35, which established as its highest priority, intelligence support to military operations. The military commander must however make a case for the priority of his or her requirement if resources not assigned or organic to his or her command are needed to fulfill the requirement.

(1) The DIA, in its support role to the JCS, prepares a listing of intelligence priorities for strategic planning for JCS publication and validates the intelligence requirements of the Services. A prioritized list of both long-term and short-term national interests is established by the NSC and passed to the CIA. There a determination is made as to whether sufficient intelligence exists

to fulfill the requirement or whether additional intelligence is needed. If it is, detailed prioritized requirements are passed to the DCI's Community Management Staff for collection tasking.

(2) All collection operations are conducted in response to validated requirements for the production of finished intelligence. The CMS tasks its members for collection to fulfill prioritized requirements. The selection of the specific collection resource rests with the department or the program manager. The management aspects of collection involve ensuring that the assets selected are the most cost-effective that can fulfill the requirement on a timely basis.

(3) Collection operations tasked by the DIA in response to DOD-generated requirements are normally conducted on an all-source, common-service basis. Conduct of intelligence operations at the tactical level to directly support the commander's immediate needs is usually accomplished by assigned or supporting intelligence organizations. Tactical commanders obtain most information on their areas of operation from assigned or supporting assets including MI units, artillery, cavalry, aviation, and maneuver units in contact. Tactical commanders leverage national capabilities by placing small numbers of tactical force intelligence soldiers at key nodes in the intelligence system to provide direct response to supported commanders' requirements. Additional information and intelligence on the area of interest is provided from higher echelons.

b. Analysis and production management. National intelligence production is the responsibility of the DCI and is exercised through the CIA's Directorate of Intelligence, which establishes schedules and priorities for all national intelligence production. Further, the directorate retains the resources and capability to produce intelligence assessments that are not coordinated with other elements of the IC.

(1) The Deputy to the DCI for National Intelligence is the principal adviser to the DCI on the production of national intelligence, both as to the manner in which it is accomplished and what it contains. The Deputy is responsible for organizing national efforts to assess and evaluate foreign intelligence data in support of intelligence objectives established by the NSC. The Deputy is the head of the Directorate of Intelligence and oversees production generated in response to standing requirements, new requirements, or as the need is perceived.

(2) No single intelligence product format meets the needs of all consumers. It is necessary to have a continuing dialogue between the consumer and the producer of intelligence while assuring that the consumer does not influence the conclusions of the final product.

(3) The most prestigious intelligence product is the President's Daily Brief (PDB), which is prepared by the Directorate of Intelligence for DCI approval and forwarding to the President. The PDB may be considered as the DCI's principal daily report to the President. Other national reports include the national intelligence brief and the Military Intelligence Digest. national intelligence estimates and similar publications are reviewed by the NFIB prior to submission to the DCI for approval and subsequent dissemination.

(4) Individual departments and agencies establish their own production schedules and priorities for the production of departmental intelligence. The DIA establishes production schedules in the DOD and distributes responsibilities among the unified and specified commands.

(5) The DIA Directorate for Analysis and Production produces, or manages the production of, all-source military intelligence to support the policy, planning, and operational requirements of the Office of the Secretary of Defense (OSD), JCS, the Services, and the combatant commands. As the DOD Production Functional Manager, the Directorate for Analysis and Production ensures that DOD intelligence production requirements are articulated; resources

are programmed and executed in compliance with national and DOD guidance; and programs are re-evaluated as missions, technical capabilities, and threat environment change.

SECTION III

DEFENSE AND ARMY INTELLIGENCE AND USES OF INTELLIGENCE

18-7. Department of Defense

The DOD is the nation's largest user of intelligence information and the largest investor in intelligence programs. The DOD has an overriding responsibility to support commanders at all levels.

a. Secretary of Defense. The SecDef exercises full direction, authority, and control over the intelligence activities of the DOD. Effective performance of DOD missions depends upon the collection, analysis, production, and dissemination of timely, relevant, accurate, synchronized, and predictive intelligence on the capabilities and intentions of foreign powers.

(1) Defense intelligence, as part of the IC, is faced with a growing number of challenges to the successful accomplishment of its defense intelligence mission. The international environment has grown more complex. Changing political alignments and instability, growing economic interdependence, nationalistic tendencies and ethnic rivalries, increased international terrorism and transnational threats, international narcotics trade, and so forth, have resulted in more diverse intelligence requirements. A significant challenge is presented by trying to collect against targets protected by relatively sophisticated command, control and communications systems, which are readily available to even the poorest countries.

(2) To strengthen the DOD performance of its intelligence functions, on 15 March 1991 the SecDef approved a plan for restructuring defense intelligence. Among other changes, the DOD reorganization of defense intelligence resulted in the consolidation of existing unified and major or joint combatant commands and component intelligence processing, analysis, and production activities into joint intelligence centers and joint analysis centers, and the consolidation of the various intelligence commands, agencies, and elements into a single intelligence command/agency within each Service.

b. Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) (OASDC3I). The ASD(C3I) has as a principal duty the overall supervision of command, control, communications, and intelligence affairs of the DOD. The ASD(C3I) is the DOD principal staff assistant for the development, oversight, and integration of DOD policies and programs relating to the strategy of information superiority for the DOD. He or she is responsible for providing capabilities that enable the U.S. military forces to generate, use, and share the information necessary to survive and succeed in accomplishing national security missions.

c. Defense Intelligence Agency (DIA). The Director, DIA is responsible for satisfying the foreign military requirements (less cryptologic) of the SecDef, OSD, CJCS, Office of the Joint Chiefs of Staff (OJCS), Joint Staff, CINCs, major DOD components, and other U.S. Government agencies, allied governments, and coalition partners (when required), and has been designated by the CJCS as a DOD combat support agency. DIA provides defense intelligence contributions to national intelligence estimates and production capabilities. The Director, DIA is a member of the National Foreign Intelligence Board and is the DOD intelligence collection manager. DIA produces, or through tasking and coordination, ensures the production of foreign military and military-related intelligence. The Director, DIA works extensively with the Services to provide support that meets a wide variety of needs. To provide daily support to the combatant commands

and U.S. Forces Korea, NATO, and Supreme Headquarters Allied Powers Europe (SHAPE), DIA initiated on-site liaison elements managed by an experienced senior civilian intelligence officer. These liaison elements, called Defense Intelligence Support Offices, expedite actions and communications between the Agency and the commands.

(1) To provide tailored support to a joint force commander, DIA can deploy national intelligence support teams (NIST) composed of DIA, NSA, and CIA personnel as well as personnel from other organizations, as required. The NIST deploys with its organic support capability and provides critical on-site intelligence connectivity between the supported command and Washington to ensure receipt of national-level intelligence. Cooperative Service efforts go into the GDIP and the Joint Military Intelligence Program, providing a broad range of recommendations to improve future intelligence capabilities. DIA also shares or provides intelligence support to the President, National Security Council Staff, National Warning Staff, Departments of Energy/State/ Treasury/ and Commerce, and the National Imagery and Mapping Agency. The DIA provides central management for the Central MASINT Organization and operates the Defense HUMINT Service, with its subordinate Defense Attaché System and HUMINT Operating Bases. DIA also operates the Joint Military Intelligence College.

(2) The Military Intelligence Board (MIB), chaired by the Director of the DIA and composed of the senior intelligence officers of the U.S. Army, U.S. Air Force, U.S. Navy, and U.S. Marine Corps, advises the SecDef and Defense agencies on matters pertaining to military intelligence. The concerns of the combatant commands are represented by DIA's Directorate for Intelligence which functions as the J2, Joint Staff. The MIB serves as the senior "Board of Governors" for intelligence organization in DOD and advises the SecDef, CJCS, Military Service Chiefs, CINCs, and defense agencies on matters pertaining to military intelligence. The Director DIA seeks consensus across the intelligence community through the MIB process.

(3) The DIA supervises the DOD Indication and Warning System and provides support to the National Military Command Center through the National Military Joint Intelligence Center (NMJIC). The DIA has the responsibility to satisfy the DOD intelligence collection requirements and to coordinate and review activities of the DOD collection resources not assigned to the DIA.

d. National Security Agency (NSA) and Central Security Service. The Director of the NSA is the Chief of the Central Security Service and manages the Consolidated Cryptologic Program, the largest single program in the National Foreign Intelligence Program. The Director is responsible for the operations of an effective unified organization for SIGINT activity. This responsibility requires extensive interaction, coordination, and cooperation with the Services and other national intelligence agencies. No other department or agency may engage in such activity without a delegation of authority by SecDef. NSA's SIGINT activities are extremely sensitive and are normally handled in special channels available to specifically designated personnel in direct support of military commanders, operations, and national foreign intelligence collection requirements. The NSA's SIGINT collection, processing, and dissemination activities involve both positive and CI information and are in direct support of military commanders and military operations and responsive to national foreign intelligence requirements.

(1) The Director of the NSA is responsible for the research and development required to meet the needs for SIGINT and communications security (COMSEC). The Director is the executive agent for executing the responsibilities of the SecDef for the COMSEC of the Government. The Director also has oversight of the Defense Cryptologic Program that lies outside the National Foreign Intelligence Program, and is responsible for providing cryptologic training and training support to the Services.

(2) In addition, the NSA was given the additional mission of information security, which, in turn, has two components—communications security and computer security.

e. National Imagery and Mapping Agency (NIMA). The NIMA was established on 1 October 1996 to address the expanding requirements in the areas of imagery, IMINT, and geospatial information.

(1) The NIMA consolidated to the extent practicable all functions of the Defense Mapping Agency. These include defense mapping, charting, and geodetic operations; production, source data storage and retrieval, and management of distribution facilities; and supervision of the Hydrographics/Topographic Center and the Defense Mapping School. NIMA also incorporated all functions of the Central Imagery Office. NIMA develops and makes recommendations on national imagery policy and is chartered to ensure responsive imagery support to the DOD, the Central Intelligence Agency, and other Federal Government departments. The NIMA tasks and evaluates imagery elements of the DOD in meeting national intelligence requirements and ensures imagery systems are exercised to support military forces.

(2) Within the DOD, the NIMA establishes the architectures for imagery tasking, collection, processing, exploitation, and dissemination. The NIMA has responsibility for establishing standards for imagery systems for which the DOD has responsibility, and ensures compatibility and interoperability of these systems. Standards for training of personnel performing imagery tasking, collection, processing, exploitation, and dissemination functions are established by the NIMA. The NIMA also supports and conducts research and development activities related to this imagery function. The NIMA serves as the functional manager for the Consolidated Imagery Program within the National Foreign Intelligence Program and for the Tactical Imagery Program (tactical intelligence and related activities). The SecDef and the Director of Central Intelligence are advised by the NIMA on future needs for imagery systems.

f. National Reconnaissance Office (NRO). The National Reconnaissance Office (NRO) is the single, national program to meet U.S. Government needs through spaceborne reconnaissance. The NRO is an agency of the DOD. The Deputy Secretary of Defense, as recommended by the Director of Central Intelligence, declassified its existence on 18 September 1992. The mission of the NRO is to ensure that the U.S. has the technology and spaceborne assets needed to enable U.S. global information superiority. This mission is accomplished through research, development, acquisition, and operation of the nation's intelligence satellites. The NRO's assets collect intelligence to support such functions as indications and warning, monitoring of arms control agreements, military operations and exercises, and monitoring of natural disasters and other environmental issues.

g. Defense Security Service (DSS). The Defense Investigative Service was established in 1972 to consolidate all DOD personnel security investigations and industrial security oversight within one agency and thereby reduce resource requirements, increase managerial efficiency, and provide a more prompt response to overall defense needs for personnel security investigations. As a result of the recent Defense Reform Initiative, the Defense Investigative Service was renamed the Defense Security Service (DSS) in November 1997 to reflect its broader security mission within the DOD. The new DSS includes the DOD Polygraph Institute, the Personnel Security Research Center and the DOD Security Institute.

18-8. Army intelligence system

The Secretary of the Army has delegated to the Under Secretary of the Army responsibility for the general supervision of the intelligence, CI, investigative, and intelligence oversight activities of the Army. The intelligence and CI elements of the military Services are responsible for the

planning, direction, collection, processing, and dissemination of military and military-related intelligence, including information on indications and warnings, foreign capabilities, plans and weapons systems, and scientific and technical developments. . See Figure 18-3 for a simplified organization of the Army intelligence system. The conduct of CI activities and the production and dissemination of CI studies and reports is a Service responsibility as are the development, procurement, and management of tactical intelligence systems and equipment; the conduct of related research, development, and test and evaluation activities; the development of intelligence doctrine; and the training of intelligence personnel.

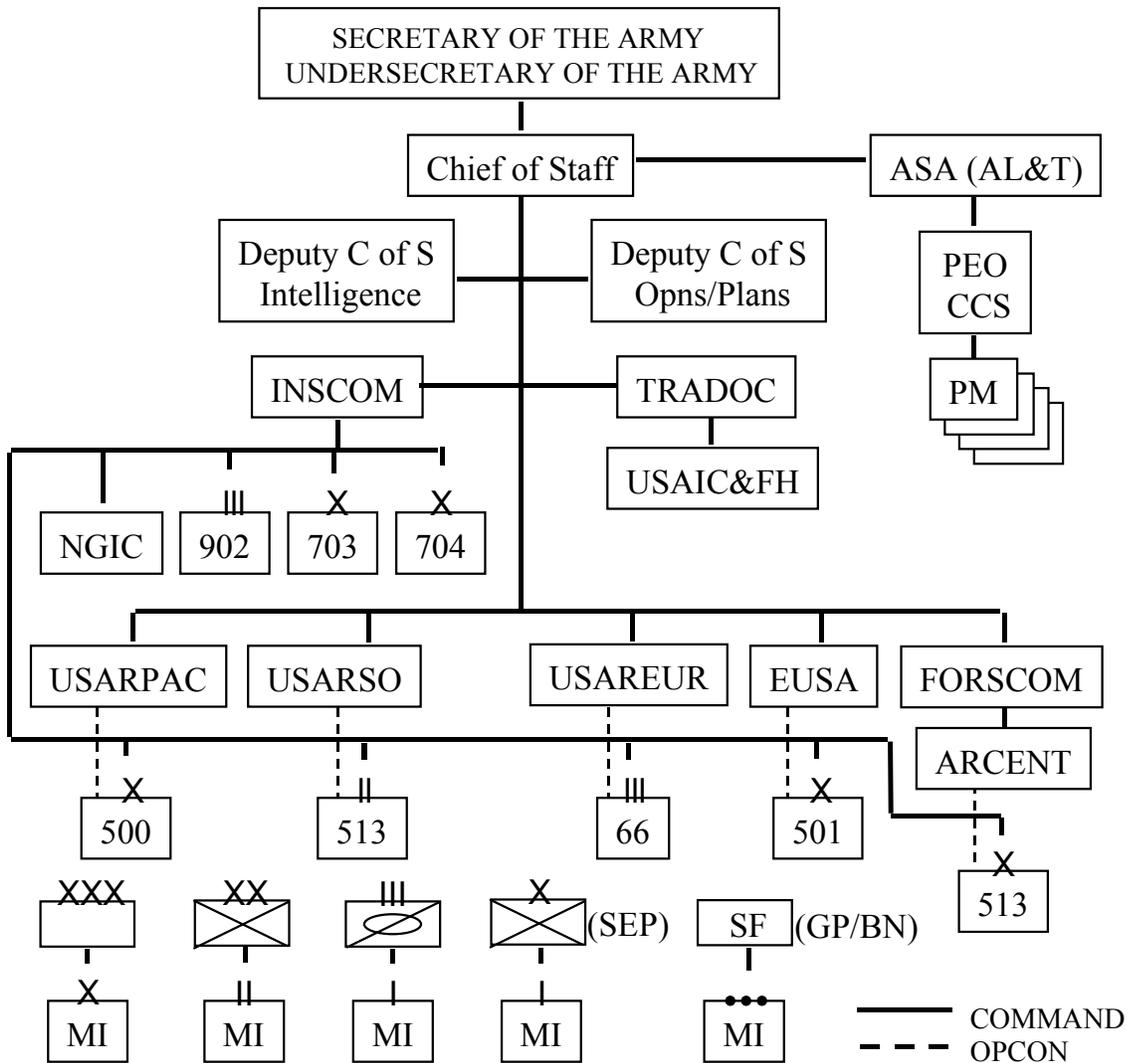


Figure 18-3. Army Intelligence Organization

a. Deputy Chief of Staff for Intelligence (DCSINT). The DCSINT is the senior intelligence officer in the U.S. Army and is responsible to the Chief of Staff for the policy formulation, planning, programming and budgeting (shared with the Deputy Chief of Staff for Programs (DCSPRO) for JMIP and TIARA), management, propriety and overall coordination of the intelligence and CI activities of the Army. The DCSINT has general staff responsibility for intelligence, CI, intelligence automation, signals intelligence, IMINT, MASINT, censorship, threat validation, intelligence collection, security, meteorological, topographic, and space activities; and monitors Army intelligence training, force structure, and readiness for both the Active Army and Reserve Components. The DCSINT, under the general guidance and tasking of

DIA, exercises general staff supervision over Army and Army-supported Intelligence Data Handling System resources and over all-source intelligence production within the Army. The DCSINT is responsible for Major Force Program 31 (Intelligence) within the Army. The DCSINT is also responsible for the Army's input into the DOD Consolidated Cryptologic Program; the General Defense Intelligence Program; the Foreign Counterintelligence Program; the Defense Joint Counterintelligence Program and Service funded programs supporting the Army Security and Intelligence Activities Program. In addition, the DCSINT is responsible for the Army input to TROJAN, foreign language sustainment, imagery dissemination, unique MI skill sustainment for Active Army and Reserve Component soldiers, Personnel Security Investigations; and is the Army SIGINT focal point. The DCSINT participates in Army Program Objective Memorandums (POMs) building by providing advice to senior program managers on ranking of intelligence requirements. Moreover, the DCSINT coordinates top intelligence requirements with major Army commands during submission of the POM assessments.

(1) The DCSINT also shares management, in the Department of the Army, with the Assistant Secretary of the Army (Manpower and Reserve Affairs) for the Defense Civilian Intelligence Personnel System (DCIPS) (formerly known as the Civilian Intelligence Personnel Management System). DCIPS is an excepted service personnel management system for the management of intelligence and intelligence-related civilian personnel throughout the DOD.

(2) The baseline document for the management of intelligence and electronic warfare (IEW) within the Army is the Army Intelligence Master Plan (AIMP). The AIMP is a requirements-based, threat- and technology-driven, comprehensive developmental strategy for the future. It is not constrained by fiscal or force structure resources. The AIMP, supported by the Assistant Secretary of the Army (Research, Development, and Acquisition) developed IEW Program Plan for the research, development, and acquisition of IEW systems, provides the basis for the development of the force structure and the fiscally constrained IEW annex of the Army modernization plan (AMP) by the Deputy Chief of Staff for Programs (DCSPRO), DA. The IEW Annex of the AMP implements the Army's force modernization principles and is the key planning document in providing long-term continuity of effort within the IEW functional area.

b. Intelligence and Security Command (INSCOM). INSCOM, a major Army command, provides a single commander for those Army intelligence and electronic warfare (IEW) units that operate at echelons above corps (EAC). INSCOM units, which are located both in CONUS and at many overseas locations, support requirements across the operational continuum. The operations of INSCOM units include: planning and direction, collection, processing, production and dissemination of all-source, multidiscipline intelligence.

(1) In each major overseas area, a military intelligence brigade or group provides multidisciplined IEW support to Army EAC and joint commanders in theater, reinforces MI units organic to operational and tactical commands at the echelons below corps, and satisfies tasking from national and departmental authorities for SIGINT, IMINT, TECHINT, MASINT, tactical HUMINT, and CI operations in response to strategic, operational, and tactical requirements. These activities are pursued through a multidisciplined force projection brigade concept.

(2) In CONUS, single and multidiscipline INSCOM MI brigade units and other organizations, some of them strategically deployable for contingencies, provide a wide range of collection capabilities as well as threat analysis, security, and OPSEC support to national and departmental agencies, contractors for sensitive projects and systems, and CONUS-based tactical consumers, including Forces Command units and the Army component of the United States Central Command. INSCOM also plays a significant role in training at the National Training

Center and with its Readiness Training (REDTRAIN) Program, which supports maintenance and development of intelligence skills in EAC and echelons below corps MI units. Finally, INSCOM supports the Training and Doctrine Command (TRADOC) in the EAC IEW combat-development process with doctrinal and force structure input, and is a materiel developer for certain specialized types of intelligence-related materiel.

c. U.S. Army National Ground Intelligence Center (NGIC). The National Ground Intelligence Center (NGIC), subordinate to INSCOM, as the Army's production center for the DOD Shared Production Program, provides basic ground intelligence to U.S. Government agencies and decision makers. NGIC produces all-source scientific, technical, and general military intelligence on foreign ground forces capabilities and systems in support of Army Title 10 requirements. This intelligence supports customers at all echelons, including Army and DOD force planners, wargamers, doctrinal developers, force modernizers, warfighters and theater joint intelligence centers with a wide range of futures-oriented threat assessments. The NGIC key products and production programs include order-of-battle and tables of organization and equipment for foreign ground forces, projection out 20 years; detailed assessments of future threats tactical/operational capabilities; conflict scenarios; and forecast of future regions of conflict of interest to U.S. force planners. The NGIC also provides threat documentation for Army research and development (R&D) and procurement programs. These products and programs require collection (MASINT and multidisciplinary collection); all-source analysis, production integration; and requirements management.

18-9. General uses of intelligence

Intelligence must quickly reach, or be accessible, to leaders and their staffs who require it to plan, prepare, execute, and assess operations. Commanders, G2s/S2s, action officers, and managers must develop a broad understanding of what intelligence they need; what can be reasonably obtained; and how it can be beneficial in the development of their programs. They must clearly state, and if possible, prioritize their intelligence requirements to the appropriate organization. Along with the development of capability based forces and systems to meet needs in the 21st century, the following are a few examples of program areas in which intelligence can have a significant impact.

a. Organizational design and force structure. Force structure designers must consider the multiplicity of the threats and must also include non-threat factors such as the deployment capabilities and limitations of allied forces. There must also be balance between the greatest threat or enemy capability and the most imminent threat in the development of a force structure. The force planner must include intelligence participation in every phase of his or her planning and decision-making. To do this, he or she must be aware of the intelligence support available and how to task the system.

b. Materiel acquisition and force modernization. The product/project/program manager must consider technical developments in foreign countries, new foreign weapons systems and countermeasures developments and future developments, as well as terrain and weather considerations. This includes an assessment of how an adversary may react to the development of a new, friendly system. The product/project/program manager must have the latest intelligence available which could affect his or her product/project/program. He or she must make the intelligence systems aware of his or her intelligence needs.

(1) The combat developer must also be aware of technical developments and must work closely with the materiel developer to ensure that a product/project/program will counter or surpass assessed threat capabilities. Both must be prepared to amend a product/project/program

prior to its completion to counter a new threat capability. Intelligence requirements are not limited to hostile forces.

(2) Technological breakthroughs in friendly or neutral nations must also be factored into materiel acquisition planning. Managers of systems of breakthrough technology must use available intelligence support to protect characteristics of the developing system as a measure of OPSEC in the R&D arena.

(3) In addition to the intelligence needs stated, the product/project/program manager must also have high quality up-to-date intelligence on the foreign collection threat directed at his or her product/project/program. Threats from both foreign government and non-government sponsored collection make up this category. These threats must be identified, collected against, and neutralized by CI assets on behalf of the materiel developer. It is important to keep the Army materiel development community continually aware of and safe from technological loss from foreign directed and controlled collection services. This strengthens the Army's technical base against illegal technology transfer and markedly improves the Army's ability to maintain technological superiority.

(4) Other factors that should be taken into account in these processes include long-range planning and consideration of opponent's strengths, weaknesses, and vulnerabilities. As the rate of technological growth continues to increase and as the threat becomes harder to define, materiel developers lean toward generic threats defined in technical terms, thereby avoiding the potential trap of being locked to a specific adversary or region.

c. Doctrine and training systems development. Doctrine and training decisions must be based on sound intelligence. Foreign military capabilities and deployments are dynamic, and U.S. Army doctrine and training decisions must be equally dynamic. To be effective in battle, U.S. soldiers must know the enemy, including the enemy's doctrine, tactics, equipment, strengths, weaknesses, and vulnerabilities, and if possible, the enemy's intentions. Doctrine and training development and implementation must be closely tied to materiel systems management. Training to operate in a hostile information warfare environment anywhere in the world places a heavy emphasis on learning about a broad range of technical command and control capabilities. Future adversaries may employ combinations of hostile, friendly, and neutral command and control systems, as well as commercial products.

d. Information operations (IO). The capability to execute IO places an increased demand on intelligence to identify rapidly and accurately both friendly and enemy vulnerabilities. Although IO is an operations function, intelligence is an integral part of the IO planning and execution actions that will degrade an adversary's use of information while protecting those of friendly forces. Successful IOs require a thorough and detailed intelligence preparation of the battlespace (IPB). IPB includes, but is not limited to, information about enemy/threat capabilities, decision-making style, information systems, considerations about the effects of: the media and the attitudes; culture; economy; demographics; politic system and parties; governmental systems and leaders; criminal organizations; and personalities of people in the area of operations.

(1) IOs are actions taken to affect adversary, and influence others' decision-making processes, information, and information system while protecting one's own information systems. IO are primarily shaping operations that create and preserve opportunities for decisive operations and sustaining operations. IOs are both offensive and defensive in nature. Successful IO influences the perceptions, decisions, and will of enemies, adversaries, and others in the area of operations, this includes the local population, displaced persons, and civil leaders. Offensive IO's

desired effects are to destroy, degrade, disrupt, deny, deceive, exploit, and influence enemy functions. Defensive IO protects friendly access to relevant information while denying adversaries and enemies the opportunity to affect the friendly information and information systems. The elements of IOs are—

- Military deception.
- Counterdeception.
- Operations security.
- Physical security.
- Electronic warfare.
 - Electronic attack.
 - Electronic protection.
 - Electronic warfare support.
- Information assurance.
- Physical destruction.
- Psychological operations.
- Counterpropaganda.
- Counterintelligence.
- Computer network operations.
 - Computer network attack.
 - Computer network defense.
 - Computer network exploit.

(2) Related IO activities are public affairs (PA) and civil affairs (CA). PA and CA are related IO activities that are distinct from IO because they do not manipulate or distort information; their effectiveness stems from their credibility with the local populace and news media. PA and CA link the force, the local populace, and the news media.

(3) In FY95, the Army organized and activated the Land Information Warfare Activity (LIWA) within the Intelligence and Security Command to assist the land component commander deal with the complexities of command and control warfare planning and execution. Tasked by the Deputy Chief of Staff for Operations (DCSOPS), HQDA, LIWA, patterned after the Joint Command and Control Warfare Center deploys tailored field support teams to specific land component commands during exercises, contingency planning, and operations. LIWA provides technical expertise and operational connectivity with other organizations and agencies supporting command and control warfare operations.

e. Support to the tactical commander. Commanders use IEW support to anticipate the battle, understand the battlespace, and influence the outcome of operations. The preeminent function of Army intelligence is to support the tactical commanders' decision-making process. The tactical commander drives the Army intelligence effort; the G2/S2 and the intelligence unit commander, are responsible for planning and directing, collecting, processing, analyzing and producing, and disseminating intelligence within the command. At corps, division, armored cavalry regiment, separate brigade, and special operations forces group/battalion, a MI unit is organic to the command, as shown in Figure 18-3. The MI unit commander plays an integral part in the intelligence mission through his or her command and control of collection operations and by training and maintaining the organic and attached intelligence assets. Additional assets leverage national, theater, sister Service, and other intelligence systems to provide intelligence to

the tactical commanders at all echelons. FM 34-1, *Intelligence and Electronic Warfare Operations*, the keystone intelligence manual, expands upon FM 100-5, *Operations*, and provides details on the doctrinal foundations for IEW operations and the employment of tactical MI units.

f. Reserve Component (RC) support. The Reserve Components (RC) participate with Active Army MI units at all echelons and are involved in virtually every aspect of military intelligence operations. In certain areas, USAR and National Guard MI capabilities, that is scientific & technical analysis, political-military estimates, substantive basic intelligence, are equal to, or even exceed, those in the active force. This phenomenon can be attributable to the fact that many MI reservists, officer and enlisted, are professional civilian intelligence employees of the national intelligence and reconnaissance agencies, the Services' intelligence departments and agencies, federally funded research centers, colleges and universities, and other U.S. Government departments performing similar activities. Consequently, their exposure to, and involvement in, intelligence operations on a daily basis rival their uniformed counterparts. The RC's contributions to filling the Army's linguist requirements are critical. The RC MI force is in the process of increasing its capacity for timely response to intelligence production requirements. RC MI centers across the country are now connected to DOD telecommunications networks. This connectivity allows RC MI units and soldiers to receive tasks from Active Army intelligence organizations, perform research and analysis within DOD databases, and file production reports back to the AA organization—all within a relatively short time. RC MI is moving rapidly to a force architecture that will integrate it more fully into the operational capabilities of the Active Army, making the Reserve Components an increasingly valuable partner.

SECTION IV

SUMMARY AND REFERENCES

18-10. Summary

Intelligence is vital to preserving the national security of the United States, and to the accomplishment of U.S. national and military security objectives. The U.S. intelligence organizations and management will continue to transform at every level to meet the needs of U.S. policy officials and military leaders faced with the uncertain environment of the 21st century and the demands of a knowledge oriented era.

18-11. References

- a.** Title 10, United States Code.
- b.** Executive Order 12333, *United States Intelligence Activities*, 4 December 1981.
- c.** Fact Sheet, The PDD on CI 21, *Counterintelligence for the 21st Century*, January 5, 2001.
- d.** Director of Central Intelligence Directive 2/9, *Management of National Imagery Intelligence*.
- e.** White House Press Briefing, 10 March 1995.
- f.** DOD Directive 5105.21, *Defense Intelligence Agency*.
- g.** DOD Directive 5105.56, *Central Imagery Office*.

- h.** DOD Directive 5137.1, *Assistant Secretary of Defense, Command, Control, Communications and Intelligence.*
- i.** Joint Publication 1-02, *DOD Dictionary of Military and Associated Terms.*
- j.** Joint Publication 2-02, *National Intelligence Support to Joint Operations.*
- k.** Army Regulation 381-10, *U.S. Army Intelligence Activities.*
- l.** Field Manual 34-1, *Intelligence and Electronic Warfare Operations.*
- m.** Field Manual 34-8, *Combat Commander's Handbook on Intelligence.*
- n.** Field Manual 34-37, *Strategic, Departmental and Operational IEW Operations.*
- o.** DIA Pub Vector 21, *The Defense Intelligence Agency Strategic Plan.*
- p.** TRADOC Pam 525-5, *Force XXI Operations.*
- q.** TRADOC Pam 525-69, *Concept for Information Operations.*
- r.** TRADOC Pam 525-75, *Intel XXI-A Concept for Force XXI.*