Joint Publication 2-01

Joint and National Intelligence Support to Military Operations

7 October 2004

PREFACE

1. Scope

This publication establishes doctrinal guidance on the provision of joint and national intelligence products, services, and support to military operations. It describes the organization of joint intelligence forces and the national Intelligence Community, intelligence responsibilities, command relationships, and national intelligence support mechanisms. It provides information regarding the fundamentals of intelligence operations and the intelligence process, discusses how intelligence supports joint and multinational planning, and describes intelligence dissemination via the global information grid.

2. Purpose

This publication has been prepared under the direction of the Chairman of the Joint Chiefs of Staff. It sets forth doctrine to govern the joint activities and performance of the Armed Forces of the United States in joint operations and provides the doctrinal basis for interagency coordination and US military involvement in multinational operations. It provides military guidance for the exercise of authority by combatant commanders and other joint force commanders (JFCs) and prescribes doctrine for joint operations and training. It provides military guidance for use by the Armed Forces in preparing their appropriate plans. It is not the intent of this publication to restrict the authority of the JFC from organizing the force and executing the mission in a manner the JFC deems most appropriate to ensure unity of effort in the accomplishment of the overall mission.

3. Application

a. Doctrine and guidance established in this publication apply to the commanders of combatant commands, subunified commands, joint task forces, and subordinate components of these commands. These principles and guidance also may apply when significant forces of one Service are attached to forces of another Service or when significant forces of one Service support forces of another Service.

b. The guidance in this publication is authoritative; as such, this doctrine will be followed except when, in the judgment of the commander, exceptional circumstances dictate otherwise. If conflicts arise between the contents of this publication and the contents of Service publications, this publication will take precedence for the activities of joint forces unless the Chairman of the Joint Chiefs of Staff, normally in coordination with the other members of the Joint Chiefs of Staff, has provided more current and specific guidance. Commanders of forces operating as part of a multinational (alliance or coalition) military command should follow multinational doctrine

and procedures ratified by the United States. For doctrine and procedures not ratified by the United States, commanders should evaluate and follow the multinational command's doctrine and procedures, where applicable and consistent with US law, regulations, and doctrine.

For the Chairman of the Joint Chiefs of Staff:

T. J. KEATING
Vice Admiral, USN
Director, Joint Staff

SUMMARY OF CHANGES

REVISION OF JOINT PUBLICATION 2-01, DATED 20 NOVEMBER 1996 (INCLUDES CONSOLIDATION OF JOINT PUBLICATION 2-02, NATIONAL INTELLIGENCE SUPPORT TO JOINT OPERATIONS, DATED 28 SEPTEMBER 1998)

- **Adds a discussion of intelligence and the challenges of the 21st century.**
- **Provides a comprehensive, updated discussion of joint and national intelligence organizations, responsibilities, and procedures.**
- **Changes the concept of "intelligence cycle" to "intelligence process."**
- **Discusses the relationship between essential elements of information and priority information requirements.**
- **Covers intelligence federation planning guidance.**
- **Introduces intelligence, surveillance, and reconnaissance (ISR) concept of operations and ISR visualization.**
- **Discusses ISR resource allocation based on validated intelligence collection requirements.**
- **Changes "production" to "analysis and production" as an intelligence operation and discusses the conversion of information into intelligence.**
- **Changes "dissemination and evaluation" to "dissemination and integration" as an intelligence operation and discusses the integration of intelligence and operations.**
- **Adds "evaluation and feedback" as an intelligence operation.**
- **Revises the discussion of intelligence support to joint planning.**
- **Discusses intelligence and the Global Information Grid.**
- **Adds an appendix on national intelligence capabilities.**
- **Promulgates definitions of "battlespace awareness," "ISR," "ISR visualization," "persistent surveillance," and "threat warning."**

Intentionally Blank

TABLE OF CONTENTS

Intentionally Blank

EXECUTIVE SUMMARY
COMMANDER'S OVERVIEW

- **Explains the Role of Intelligence in Military Operations**
- **Describes Joint and National Intelligence Organizations, Responsibilities, and Support Mechanisms**
- **Discusses Intelligence Operations and the Intelligence Process**
- **Describes Intelligence Support to Joint Planning**
- **Discusses Intelligence and the Global Information Grid**

Introduction

The objective of joint intelligence operations is to integrate Service and national intelligence capabilities into a unified effort that surpasses any single organizational effort and provides the most accurate and timely intelligence to commanders.

Joint intelligence is produced by elements of more than one Service and consequently relies heavily on the timely and integrated departmental intelligence afforded by national intelligence organizations. **This joint intelligence effort facilitates that degree of dominance in the information domain which permits the conduct of operations without effective opposition (i.e., information superiority).** In order to accomplish this, intelligence must provide the joint force commander (JFC) with as timely, complete, and accurate an understanding as possible of the battlespace. Intelligence staffs must anticipate and fully understand the intelligence requirements of their superior and subordinate commands and components, identify organic intelligence capabilities and shortfalls, access theater and/or national systems to alleviate shortfalls, and ensure that timely and appropriate intelligence is provided or available to the JFC and subordinate commands and components.

Intelligence Support to Military Operations

Intelligence plays a critical role across the range of military operations.

Commanders use intelligence to anticipate the battle, visualize and understand the full spectrum of the battlespace, and influence the outcome of operations. Intelligence enables commanders at all levels to focus their combat power and to provide full-dimensional force protection across the range of military operations. **In war**, intelligence focuses on adversary military capabilities, centers of gravity (COGs), and potential courses of action to provide operational and tactical commanders the information they need to plan and conduct operations. **Short**

of war, joint operations are normally very sensitive to political considerations and can be governed by rules of engagement requiring the adoption of a new and complex set of operational responses. The intelligence directorate of a joint staff (J-2) must modify and tailor intelligence support to meet the unique challenges presented in each operation.

Joint Intelligence Organizations

Joint intelligence organizations are directly responsible for providing the combatant command and subordinate joint force with a common, coordinated intelligence picture by fusing national and theater intelligence and law enforcement/ counterintelligence information into all-source estimates and assessments.

Joint intelligence activities focus on determining the joint force's intelligence needs based on the mission and commander's guidance; prioritizing intelligence requirements; developing an optimal collection plan and strategy; identifying collection or production shortfalls that may require resource augmentation, intelligence federation, or direct national-level analytic support; and then evaluating satisfaction of needs and requirements and adjusting intelligence services and support accordingly.

The combatant command J-2 assists the commander and staff in developing strategy, planning theater campaigns, and organizing the command relationships of theater intelligence assets for effective joint, interagency, and multinational operations and to facilitate interagency coordination. Additionally, the J-2 is responsible for determining the requirements and direction needed to ensure unity of the intelligence effort supporting the commander's objectives.

The combatant command joint intelligence center (JIC) is the focal point for intelligence analysis and production effort, and is organized in a manner best suited to satisfy the combatant commander's intelligence requirements. If the JIC cannot meet the combatant commander's requirements, the JIC forwards a request for information to the National Military Joint Intelligence Center or to subordinate command levels using the community on-line intelligence system for end-users and managers.

The organizational structure of a subordinate joint force's intelligence element is determined by the JFC based on the situation and mission. All subordinate joint force J-2s, however, will at a minimum require a core element of analytical and administrative capabilities. Most situations will require augmentation of joint force intelligence capabilities through the deployment and integration of theater intelligence elements into a joint intelligence support element (JISE). Capabilities of the JISE include order of battle analysis, identification of adversary

COGs, analysis of adversary command, control, communications, and computers, targeting support, collection management, and maintenance of a 24-hour watch.

National Intelligence Organizations

National intelligence organizations conduct extensive collection, processing, analysis, and dissemination activities.

National intelligence organizations employ specialized resources and dedicated personnel to gain information about potential adversaries, events, and other worldwide intelligence requirements. These organizations routinely provide support to the JFC while continuing to support national decision makers. However, **the focus of these national organizations is not evenly split among intelligence customers and varies according to the situation and competing requirements.**

The Intelligence Community (IC) refers in the aggregate to those Executive Branch agencies and organizations that are funded in the National Foreign Intelligence Program. The IC consists of 15 member organizations:

The **Defense Intelligence Agency (DIA)** has oversight of the Department of Defense Intelligence Production Program (DODIPP), under which all-source intelligence is produced for use by both policymakers and commanders. Under DODIPP, DIA's Armed Forces Medical Intelligence Center is assigned responsibility for medical intelligence and DIA's Missile and Space Intelligence Center is responsible for missile and space intelligence. Additionally, DIAs Defense Human Intelligence (HUMINT) Service provides a full range of HUMINT and HUMINT-related intelligence collection services to combatant commanders and other Department of Defense (DOD) and national-level consumers. DIA also provides intelligence support in areas such as: counterintelligence, counterterrorism, counterdrug operations, computer network operations, personnel recovery, proliferation of weapons of mass destruction and the means of delivery, United Nations peacekeeping and coalition support, measurement and signature intelligence (MASINT), noncombatant evacuation efforts, indications and warning, targeting, battle damage assessment, current intelligence, collection management, intelligence architecture and systems support, and document and media exploitation capability.

The National Security Agency/Central Security Service is a unified organization structured to provide for the signals intelligence mission of the United States and to ensure the

protection of national security systems for all departments and agencies of the United States Government.

The National Geospatial-Intelligence Agency provides timely, relevant, and accurate geospatial intelligence support to include imagery intelligence, geospatial information, national imagery collection management, commercial imagery, imagery-derived MASINT, and some meteorological and oceanographic data and information.

The National Reconnaissance Office is responsible for integrating unique and innovative space-based reconnaissance technologies, and the engineering, development, acquisition and operation of space reconnaissance systems and related intelligence activities.

The Service Intelligence Organizations provide intelligence support for Departmental missions related to military systems, equipment, training, and national intelligence activities. The Services also provide support to DOD entities, including combatant commands and their components.

The Central Intelligence Agency's (CIA's) primary areas of expertise are in HUMINT collection, all-source analysis, and the production of political and economic intelligence.

The Department of State (DOS) Bureau of Intelligence and Research performs intelligence analysis and produces studies on a wide range of political and economic topics essential to foreign policy determination and execution.

The Federal Bureau of Investigation (FBI) has primary responsibility for counterintelligence (CI) and counterterrorism operations conducted in the United States. FBI CI operations overseas are coordinated with the CIA.

The Department of Treasury analyzes foreign intelligence related to US economic policy and participates with the DOS in the overt collection of general foreign economic information.

The Department of Energy analyzes foreign information relevant to US energy policies and nonproliferation issues.

The Department of Homeland Security's Directorate for Information Analysis and Infrastructure Protection analyzes the

vulnerabilities of US critical infrastructure, assesses the scope of terrorist threats to the US homeland, and provides input to the Homeland Security Advisory System.

The United States Coast Guard (USCG), a component of the Department of Homeland Security, operates as both an armed force and a law enforcement organization. The USCG's Maritime Intelligence Fusion Centers Atlantic and Pacific serve as the central hub for collection, fusion, analysis and dissemination of maritime intelligence and information to Coast Guard operating units, Department of Homeland Security and all members of the IC including DOD and key decision makers at the national level.

Intelligence Operations

Intelligence supports joint operations by providing critical information and finished intelligence products to the combatant command, the subordinate Service and functional component commands, and subordinate joint forces.

Commanders at all levels depend on timely, accurate information and intelligence on an adversary's dispositions, strategy, tactics, intent, objectives, strengths, weaknesses, values, capabilities and critical vulnerabilities. **The intelligence process is comprised of a wide variety of interrelated intelligence operations.** These intelligence operations (planning and direction, collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback) must focus on the commander's mission and concept of operations.

The intelligence process describes how the various types of intelligence operations interact to meet the commander's intelligence needs.

The intelligence process provides a useful model that, albeit simplistic, nevertheless facilitates understanding the wide variety of intelligence operations and their interrelationships. There are no firm boundaries delineating where each operation within the modern intelligence process begins or ends. Intelligence operations are not sequential; rather they are nearly simultaneous. Additionally, not all operations necessarily continue throughout the entire intelligence process. The increased tempo of military operations requires an unimpeded flow of automatically processed and exploited data that is both timely and relevant to the commander's needs. This unanalyzed combat information must be simultaneously available to both the commander (for time-critical decision making) and to the intelligence analyst (for the production of current intelligence assessments). Likewise, the analysis, production, and dissemination of intelligence products must be accomplished in time to support the commander's decision-making needs.

Planning and direction. Joint intelligence operations begin with the identification of a need for intelligence regarding all relevant aspects of the battlespace especially the adversary. These intelligence needs are developed by the J-2 in coordination with other staff elements, and are formalized as intelligence requirements early in the planning process. **Those critical pieces of intelligence the commander must know by a particular time to plan and execute a successful mission are identified as the commander's priority intelligence requirements (PIRs).** PIRs are identified at every level and are based on guidance obtained from the mission statement, the commander's intent, and the end state objectives.

Collection. The collection portion of the intelligence process involves **tasking appropriate collection assets and/or resources to acquire the data and information required to satisfy collection objectives.** Collection includes the identification, coordination, and positioning of assets and/or resources to satisfy collection objectives. Finally, collection involves gaining electronic, physical, spectral, or visual access to a target and searching for, discovering/sensing, and gathering characteristics, data, equipment, or phenomena to process and exploit.

Processing and exploitation. Once the data that might satisfy the requirement is collected, it must undergo processing and exploitation. **Through processing and exploitation, the collected raw data is transformed into information that can be readily disseminated and used by intelligence analysts to produce multidiscipline intelligence products.** Relevant, critical information should also be disseminated to the commander and joint force staff to facilitate time-sensitive decision making. Processing and exploitation time varies depending on the characteristics of specific collection assets.

Analysis and production. The analysis and production portion of the intelligence process involves **integrating, evaluating, analyzing, and interpreting information from single or multiple sources into a finished intelligence product.** The demands of the modern battle require intelligence products that anticipate the needs of the commander and are timely, accurate, usable, complete, relevant, objective, and available.

Dissemination and integration. **Properly formatted intelligence products are disseminated to the requester,** who integrates the intelligence into the decision-making and planning processes.

Evaluation and feedback.

Intelligence operations, activities and products are continuously evaluated. Based on these evaluations and the resulting feedback, remedial actions should be initiated, as required, to improve the performance of intelligence operations and the overall functioning of the intelligence process.

Intelligence Support to Joint Planning

In today's global threat environment, rigid sequentially-structured intelligence support to planning must yield to a more dynamic process involving overlapping and simultaneous activities.

Military planners and decision makers require a faster, more accurate flow of information and intelligence. Intelligence support in this environment requires increased agility to quickly identify requirements, collect and disseminate information, and analyze and produce predictive intelligence to support the planning process. Intelligence support to the joint planning effort must be focused to ensure that it fully anticipates and dynamically responds to the commander's requirements and the requirements of subordinate units and/or elements.

Intelligence support to joint operation planning includes a single integrated set of policies, activities, and procedures applicable to both deliberate planning and crisis action planning (CAP). Deliberate plans include operation plans in complete format, operation plans in concept format with or without time-phased force and deployment data, and functional plans. CAP is conducted for the actual commitment of allocated forces, based on the current situation, when a contingency response is imminent. This planning results in time-sensitive development of campaign plans and/or operation orders for execution.

Intelligence and the Global Information Grid

The Global Information Grid is the end-to-end integrated set of information technology capabilities, associated processes and personnel for collecting, processing, storing, disseminating and managing information on demand to commanders, policy makers and support personnel in a globally interconnected environment.

The Global Information Grid (GIG) includes **all DOD-owned and leased communications and computing systems software, data, security services, and other associated services necessary to achieve information superiority.** This environment supports all DOD and IC missions and functions (strategic, operational and tactical), in war and peace, at all operating locations (bases, posts, camps, stations, facilities, mobile platforms and deployed sites). The GIG provides interfaces to coalition, allied, and non-DOD users and systems.

The communications networks and information processing, storage, and management systems that comprise the GIG provide the basic framework for the timely transfer of data and information to support military operations. The GIG also provides the means for the timely

dissemination of information and finished intelligence to commanders and other key decision makers, thereby facilitating information superiority. The GIG architecture implements common procedures, standards, and streamlined support, and continues to evolve. **The intelligence portion of the GIG is designed to provide an architecture that can be individually tailored to the specific needs of a joint force, ensures survivability and flexibility through distributed operations, and can be rapidly reconfigured to accommodate changing demands and responsibilities including facilitating relationships among federated intelligence partners.** This tailorable, distributed, and rapidly reconfigurable joint architecture provides all relevant available battlespace information to the user in the form of a common operational picture. **Within the GIG, the Department of Defense Intelligence Information System (DODIIS) is the aggregation of personnel, procedures, equipment, computer programs, and supporting communications of the military IC.** DODIIS defines the standards for intelligence system and application interoperability. The system concept provides an integrated strategic, operational, and tactical user environment for performing identical intelligence support functions on compatible systems. DODIIS provides a robust and flexible intelligence capability for subordinate joint forces as long as supporting communications lines are available. DODIIS tools support the movement of intelligence between DIA, the combatant commands, the Services, and other intelligence production and customer activities worldwide.

Intelligence-Related Communications Infrastructure.

The joint intelligence communications subarchitecture encompasses collection, processing, exploitation, analysis, and dissemination nodes. These nodes are supported by a robust communications infrastructure and automated systems equipped with tailored applications to meet the broad array of intelligence activities. Command, Service, and combat support agency intelligence processes rely on a communications backbone consisting of the Joint Worldwide Intelligence Communications System and the Secret Internet Protocol Router Network. This infrastructure is supplemented by a distributed, common exploitation and dissemination system, tactical data links, and intelligence broadcast services.

CONCLUSION

This publication establishes doctrinal guidance on the provision of joint and national intelligence products, services, and support to military operations. It describes the organization of joint intelligence forces and the national IC, intelligence responsibilities, command relationships, and national intelligence support mechanisms. It provides information regarding the fundamentals of intelligence operations and the intelligence process, discusses how intelligence supports joint and multinational planning, and describes intelligence dissemination via the GIG.

Intentionally Blank

CHAPTER I
THE ROLE OF INTELLIGENCE IN MILITARY OPERATIONS

"When I took a decision, or adopted an alternative, it was after studying every relevant — and many an irrelevant — factor. Geography, tribal structure, religion, social customs, language, appetites, standards — all were at my finger-ends. The enemy I knew almost like my own side. I risked myself among them a hundred times, to learn."

Colonel T. E. Lawrence
Letter to Liddell Hart, 26 June 1933

1. Introduction

a. **The objective of joint intelligence operations is to integrate Service and national intelligence capabilities into a unified effort that surpasses any single organizational effort and provides the most accurate and timely intelligence to commanders.** Joint intelligence is produced by elements of more than one Service and consequently relies heavily on the timely and integrated departmental intelligence afforded by national intelligence organizations. This joint intelligence effort facilitates that degree of dominance in the information domain which permits the conduct of operations without effective opposition (i.e., information superiority). In order to accomplish this, intelligence must provide the joint force commander (JFC) with as timely, complete, and accurate understanding as possible of the battlespace, particularly all aspects of the adversary's forces, capabilities, and intentions. Intelligence staffs must anticipate and fully understand the intelligence requirements of their superior and subordinate commands and components, identify organic intelligence capabilities and shortfalls, access theater and/or national systems to alleviate shortfalls, and ensure that timely and appropriate intelligence is provided or available to the JFC and subordinate commands and components (see Figure I-1). These objectives are achieved through the cooperative and comprehensive efforts of all intelligence personnel throughout the intelligence process.

b. Joint intelligence doctrine defines the roles and relationships of intelligence organizations at the national level, in the combatant commands, and in subordinate joint forces. The National Military Joint Intelligence Center (NMJIC), the combatant command's intelligence directorates (J-2s), the joint intelligence centers (JICs) (or equivalents) of combatant commands, and the J-2s and joint intelligence support elements (JISEs) of subordinate joint forces support the commander by minimizing the number of organizations and echelons upon which the JFC must rely in order to accomplish intelligence support missions. **The goal is to maximize the impact of intelligence on military operations by increasing the efficiency of the intelligence process and the effectiveness of the intelligence organizations that support the JFC.** Robust intelligence resources, methodologies, and products for every military option and scenario should be developed, reviewed, and exercised regularly. Intelligence that is anticipatory, timely, accurate, usable, complete, relevant, objective, and available is a crucial enabler of decisive unified action and successful military operations.

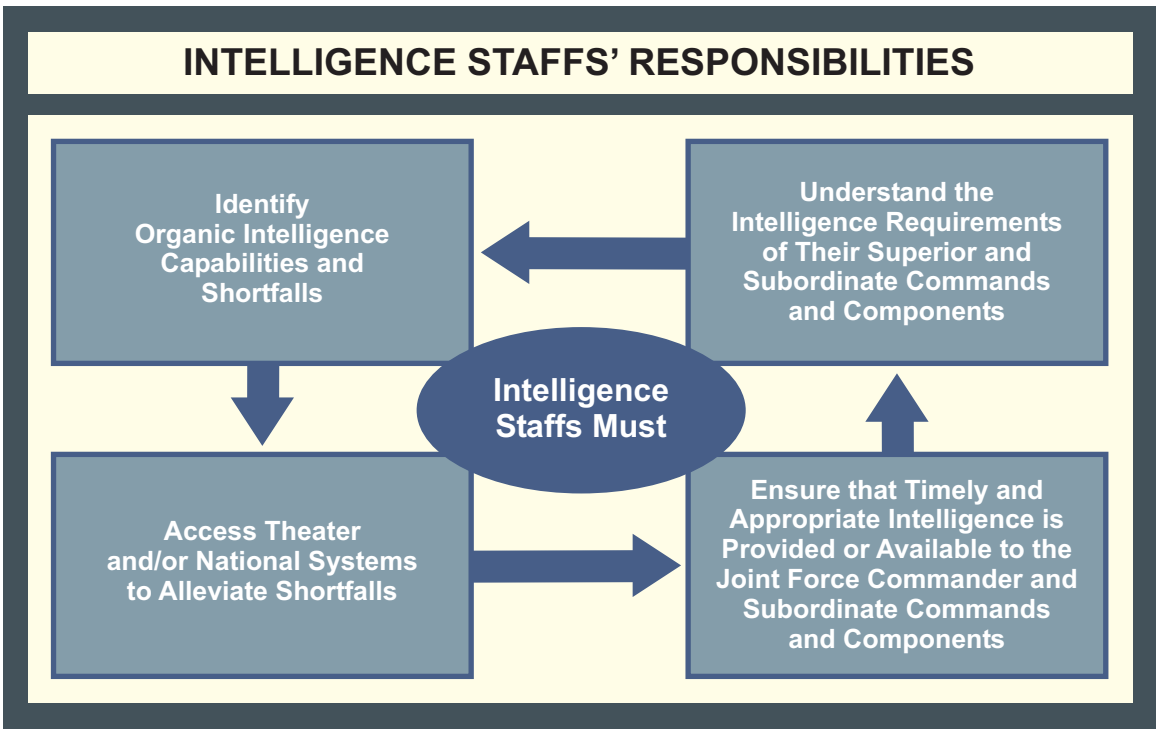


Figure I-1. Intelligence Staffs' Responsibilities

2. Intelligence and the Challenges of the 21st Century Environment

a. **The 21st century environment presents increasingly difficult intelligence challenges.** Threats now span a widening range of activities: from terrorist use of weapons of mass destruction (WMD) to regional military or social crises that threaten the territorial integrity of US allies. Some regional powers are capable of challenging US security interests in geographically diverse areas. The global availability of new technology provides regional powers with the means to rapidly develop new military capabilities without the traditional warning time associated with normal buildup indicators. The inherent deniability of dual use technologies, particularly in the chemical and biological industries, makes future technical assessments and estimates even more difficult. Transnational threats such as terrorism, computer network attack, and the global proliferation of missiles and weapons technology have reduced the relevance of traditional international boundaries while increasing the significance of "non-state actors." The use of asymmetric warfare techniques such as denial and deception has become increasingly popular among potential adversaries as a means to counter US and allied intelligence, surveillance, and reconnaissance (ISR) and power projection capabilities. Furthermore, intelligence support to military operations will be affected by non-threat-related environmental factors such as requisite changes in sources and methods and user expectations. **To meet these formidable challenges, the intelligence process must be sufficiently agile and intelligence organizations prepared and ready to respond to a myriad of anticipated and unanticipated requirements in a wide variety of situations across the full range of military operations.** At the same time, the quality of the intelligence product remains of paramount importance, and must be sufficiently detailed and timely to satisfy the commander's decision-making needs.

b. The 21st century environment also offers unparalleled technological opportunities for meeting these challenges by dramatically increasing the timeliness of relevant information and by virtually integrating operations and intelligence. Advances in data processing, such as artificial intelligence, knowledge bases, and iterative search tools, have created a new paradigm in which the timelines of intelligence operations and the intelligence process have been greatly compressed. Likewise, the traditional delineations among the various types of intelligence operations have been blurred. **Intelligence production and dissemination now occur nearly simultaneously as multimedia intelligence products resident in knowledge bases are automatically updated with new information as it is collected and processed.** Dynamic iterative search tools, virtual collaborative work environments, and a common operational picture (COP) enable intelligence personnel to **nearly simultaneously** exploit, analyze, produce and disseminate relevant information. Secure digital communication links and automated exploitation tools now make it possible to immediately process collected data and disseminate the resulting information to support the commander's decision-making needs and provides the timely feedback required to support the dynamic management of intelligence collection assets. Likewise, direct "sensor-to-shooter" connectivity dramatically increases the timeliness and precision of information required to successfully engage adversary time-sensitive targets.

"Successful employment of modern weapons systems, new operational concepts, and innovative combat techniques — particularly those involving forces that are lighter, faster, more agile, and more lethal — also depends on rapid, precise, accurate, and detailed intelligence. The persistent demand for very high-resolution intelligence data is driven by a combination of factors: the inventory of increasingly precise weaponry; a mission mix that requires surgical application of force; and growing use of high-fidelity modeling to support mission planning. In addition, future trends — such as the weaponization of information technologies or the increased probability of combat operations in urban terrain — foreshadow a dramatic growth in requirements for the fine-grained, time sensitive intelligence collection and analysis."

GEN Hugh Shelton, USA
Chairman of the Joint Chiefs of Staff, 2000

3. Intelligence Support to Military Operations

Intelligence plays a critical role across the range of military operations. Commanders use intelligence to anticipate the battle, visualize and understand the full spectrum of the battlespace, and influence the outcome of operations. Intelligence enables commanders at all levels to focus their combat power and to provide full-dimensional force protection across the range of military operations.

a. **In war**, intelligence focuses on enemy military capabilities, centers of gravity (COGs), and potential courses of action (COAs) to provide operational and tactical commanders the information they need to plan and conduct operations. It enables the JFC to visualize, understand, and identify when and where to apply combat power to exploit enemy vulnerabilities and capitalize on opportunities with minimum risk.

Joint Publication (JP) 2-0, Doctrine for Intelligence Support to Joint Operations*, describes intelligence and the range of military operations.*

INTELLIGENCE SUPPORT ACROSS THE RANGE OF MILITARY OPERATIONS

In 1992 the Defense Intelligence Agency (DIA) sought to improve support for future disaster relief operations. The initiative was largely a response to Operation SEA ANGEL, a major disaster relief operation in Bangladesh in May 1991 in which some 152,000 people were killed by a tropical cyclone. Interviews with SEA ANGEL commanders indicated they had not had adequate intelligence on Bangladesh's physical and cultural environment, infrastructure, disaster relief capabilities, and the potential for further disaster. The DIA initiative attempted to satisfy these requirements in preparing for disasters.

The most important component of this initiative was the development of a new, all-source, comprehensive finished intelligence product modeled on DIA's Contingency Support Studies (CSS) and Contingency Support Products. Such products originally were designed to provide "off-the-shelf" contingency intelligence for combat operations and noncombatant evacuation operations.

The new CSS-type product was designed for potential humanitarian relief operations generated by natural or technological disasters. In addition to the traditional essential elements of information (EEIs) included in studies that support the movement and deployment of military forces — such as transportation infrastructure intelligence — the product was designed to include EEIs that are unique and yet critical to the planning and prosecution of disaster relief operations.

SOURCE: G. Ted Constantine, Intelligence Support to Humanitarian-Disaster Relief Operations, Center for the Study of Intelligence, December 1995

b. **Short of war, joint operations** are normally very sensitive to political considerations and can be governed by rules of engagement requiring the adoption of a new and complex set of operational responses. The J-2 must modify and tailor intelligence support to meet the unique challenges presented in each operation. In addition, the nature and intensity of a potential threat can change suddenly and dramatically. For example, a peacekeeping operation may abruptly transition to a combat peace enforcement operation should any of the belligerents fail to honor the terms of the truce. Therefore, intelligence resources at every echelon should be structured to provide support that is proactive, aggressive, predictive, and flexible.

c. Across the range of military operations, intelligence provides threat assessments that are crucial to force protection and homeland defense. The timely horizontal integration and sharing of intelligence and appropriate law enforcement information among combatant commands, interagency members, and

multinational partners is vital to this effort. To achieve such an end state, the Department of Defense (DOD) works with the Department of Homeland Security and the Department of Justice to arrive at a single coherent security policy and architecture that includes personnel security policies and practices and supporting information technologies. Of particular importance to force protection is the timely sharing of counterintelligence (CI), law enforcement information, and other actionable intelligence regarding asymmetric threats from terrorism, WMD, and information operations (IO).

(1) **CI support is crucial to protecting the force and combating terrorism and must be fully integrated into operation planning and execution.** The Department of Defense CI program has four separate but interrelated functions: investigations; collection; operations; and analysis and production. All four functions will be incorporated into CI planning and support activities. CI operations are conducted to detect, identify, assess, exploit, and counter or neutralize the threat to security posed by foreign intelligence services or organizations, or by individuals engaged in espionage, sabotage, subversion, or terrorism. An effective CI program uses a multidisciplined approach that relies on the timely fusion of law enforcement information, CI, and other traditional intelligence sources to counter an adversary's all-source intelligence and other security threats. The Counterintelligence Field Activity (CIFA) and CI elements from the Service components play a lead role in this multidisciplined effort and facilitate information sharing among combatant commands, interagency partners, and law enforcement organizations.

Basic CI policy is contained in DOD Directive (DODD) 5240.2, DOD Counterintelligence. *Additional information on CI support to operations can be found in JP 2-01.2,* Joint Doctrine, Tactics, Techniques, and Procedures for Counterintelligence Support to Operations.

(2) **Intelligence is a critical enabler of our efforts to protect the force from WMD and to support counterproliferation and nonproliferation efforts.** At the strategic level, intelligence facilitates nonproliferation activities and the development of effective counterproliferation plans by providing intelligence of activities between suppliers of WMD and states and non-state actors attempting to acquire WMD, and by providing assessments of adversary WMD capabilities. Likewise, at the operational level, commanders require timely all-source, actionable intelligence to take decisive actions against WMD threats. Intelligence provides warning of WMD attacks and is vital to the identification, tracking, and interdiction of adversary proliferation attempts.

(3) Rapid and continuing advances in information technology (IT) present US forces with significant opportunities and vulnerabilities relevant to full dimensional protection. IO has become increasingly important as a tool for both assuring the flow of vital friendly information and for denying an adversary access to information. **A growing percentage of intelligence manpower, technical resources, products and efforts are dedicated to supporting IO.** Successful IO requires tailored and highly detailed intelligence analyses of a wide variety of human and information environmental factors, such as public attitudes and perceptions, leadership decision-making styles, telecommunications nodes, and sources of information.

INTELLIGENCE SUPPORT TO THE GLOBAL WAR ON TERRORISM

On 11 September 2001, members of Usama Bin Laden's al Qaida organization launched the most devastating, synchronized, terrorist attack on US soil resulting in the loss of several thousand lives. In response to this attack, Operation ENDURING FREEDOM was launched to track down and neutralize the terrorist leaders and organizations responsible for the attack. ENDURING FREEDOM provides an excellent example of an operation that spans the full range of military operations and demonstrates the need for precise, timely, and accurate information and intelligence. Specifically, Operation ENDURING FREEDOM demonstrates the importance of:

- **a rational global allocation of high demand national intelligence, surveillance, and reconnaissance (ISR) assets based on valid intelligence collection requirements;**
- **a theater ISR concept of operations based on a coherent collection strategy that fully integrates and optimizes the use of all organic, multinational, allied, commercial, and requested national ISR assets;**
- **a persistent or near-continuous battlespace surveillance capability as opposed to periodic reconnaissance;**
- **a dynamic intelligence process that delivers reliable information simultaneously to commanders (for time-sensitive decision making) and to intelligence analysts (for multi-source intelligence production);**
- **sufficient numbers of air-delivered unattended ground sensors with a wide range of capabilities;**
- **sufficient processing, exploitation, and dissemination resources to handle increased volumes of collected data;**
- **adequate planning for intelligence reachback and crisis intelligence federation;**
- **incorporation of medical intelligence from the Armed Forces Medical Intelligence Center into all-source intelligence;**
- **sufficient numbers of chemical, biological, radiological, nuclear, and high-yield explosive experts/analysts along with specialized collection, transport, and exploitation teams;**

- **sufficient numbers of in-theater human intelligence and counterintelligence personnel, area specialists, and linguists; and**

- **reachback and distributed operations in ISR processing, exploitation, and command and control.**

SOURCE: Various Sources

Intentionally Blank

CHAPTER II
JOINT AND NATIONAL INTELLIGENCE ORGANIZATIONS, RESPONSIBILITIES, AND PROCEDURES

"Nothing should be neglected in acquiring a knowledge of the geography and military statistics of their states, so as to know their material and moral capacity for attack and defense as well as the strategic advantages of the two parties."

Jomini
***Precis de l' Art de la Guerre*, 1838**

1. Overview

JFCs exercise control over an impressive array of organic and attached intelligence collection and analysis resources. Nevertheless, these alone will not be capable of satisfying all the joint force's information requirements. **The joint force J-2 will have to rely on both theater and national intelligence organizations for support in order to provide the JFC with the most accurate intelligence possible.** The resources of the NMJIC and the Defense Intelligence Agency (DIA) operational intelligence coordination center (OICC), national intelligence agency command representatives, crisis intelligence federation partners, United States Joint Forces Command (USJFCOM) quick reaction teams (QRTs), and national intelligence support teams (NISTs) provide the means to integrate national intelligence capabilities into a comprehensive intelligence effort designed to support the joint force. The J-2 must understand the organization, production responsibilities, and expertise resident in the various national intelligence agencies and supporting intelligence federation partners in order to exploit their capabilities efficiently. This is increasingly important as new technology facilitates collaborative analysis and production and blurs the traditional distinction between joint force and national-level intelligence.

SECTION A. JOINT INTELLIGENCE

2. Introduction

Joint intelligence organizations are directly responsible for providing the combatant command and subordinate joint force with a common, coordinated intelligence picture by fusing national and theater intelligence and law enforcement/CI information into all-source estimates and assessments. Joint intelligence activities focus on determining the joint force's intelligence needs based on the mission and commander's guidance; prioritizing intelligence requirements; developing an optimal collection plan and strategy; identifying collection or production shortfalls that may require resource augmentation, intelligence federation, or direct national-level analytic/collection support; and then evaluating satisfaction of needs and requirements and adjusting intelligence services and support accordingly.

3. Combatant Command Intelligence Organizations and Responsibilities

a. **Combatant Command J-2.** The combatant command J-2 **assists the commander and staff in developing strategy, planning theater campaigns, and organizing the command**

relationships of theater intelligence assets for effective joint and multinational operations and to facilitate interagency coordination. Additionally, the J-2 is responsible for determining the requirements and direction needed to ensure unity of the intelligence effort supporting the commander's objectives. The J-2 provides higher echelons, up to and including the NMJIC, and subordinate commands with a common, coordinated, all-source intelligence picture by applying national intelligence capabilities, employing joint force intelligence resources, and identifying and integrating additional intelligence resources such as the JIC and component command intelligence assets, and fusing information derived from law enforcement/CI organizations. Specifically, the combatant command J-2 will:

(1) Usually exercise staff supervision over the JIC.

(2) Determine and recommend prioritized intelligence needs based on mission analysis and commander's planning guidance, specifically priority intelligence requirements (PIRs) for projected decisions being considered by the commander.

(3) Develop and manage an optimal collection plan that fully supports, and is completely synchronized with, current and planned joint operations.

(4) Identify available intelligence resources, match those resources against requirements, and identify potential analytic or collection resource shortfalls.

(5) Request, as required, additional collection resources and analysis and production support from national intelligence organizations or federated intelligence partners.

(6) Coordinate the intelligence effort of subordinate commands.

(7) Plan and coordinate the overall joint intelligence preparation of the battlespace (JIPB) effort within the combatant command, and ensure that its JIPB analyses are fully integrated with all intelligence preparation of the battlespace (IPB) and JIPB products produced by subordinate commands and other organizations.

(8) Assist the operations directorate (J-3) in development of mission objectives and determine the availability, quality, and quantity of intelligence assessments, knowledge, and information to support the combatant commander's decisions, guidance, and intent relative to the joint mission.

(9) Recommend for the combatant commander's approval, appropriate intelligence support relationships for combatant command and component command intelligence organizations. Intelligence support relationships include:

(a) **General Support.** An intelligence element in general support will provide support to the joint force as a whole and not to any particular subordinate unit. The intelligence element responds to the requirements of the joint force as tasked by the J-2.

(b) **Direct Support.** An intelligence element in direct support provides intelligence support to a specific unit. The intelligence element is required to respond to the supported unit's intelligence requirements. As a second priority, the intelligence element will respond to the intelligence requirements of the joint force as tasked by the J-2.

(c) **Close Support.** An intelligence unit with a close support mission will provide intelligence support on targets and objectives sufficiently near the supported force as to require detailed integration and coordination with the fire, movement, or other actions of the supported unit.

(d) **Mutual Support.** Intelligence elements receive a mutual support mission when their assigned tasks, their position relative to each other, and their capabilities allow them to coordinate their activities in order to assist each other to respond to the intelligence requirements of the joint force as tasked by the J-2.

b. **Combatant Command Joint Intelligence Center.** The JIC is the focal point for the combatant command's intelligence analysis and production effort, and is organized in a manner best suited to satisfy the combatant commander's intelligence requirements**. Each combatant command possesses a JIC or JIC equivalent.** For example, United States European Command (USEUCOM) has a joint analysis center (JAC), and United States Northern Command has a Combined Intelligence and Fusion Center. Likewise, United States Forces Korea (USFK) relies on a Combined Intelligence Operations Center. If the JIC or JIC equivalent cannot meet the combatant commander's requirements, the JIC forwards a request for information (RFI) to the NMJIC or to subordinate command levels using the community on-line intelligence system for end-users and managers (COLISEUM) RFI management system. In some cases, the JIC may also seek to ensure timely support by submitting requests to intelligence community (IC) production centers through the national agency representatives to the command.

(1) **Organization.** There is no "typical" JIC organizational structure, and each JIC will vary depending on combatant command requirements.

(a) A JIC is organized in accordance with (IAW) the combatant commander's prerogatives as specified in the command's intelligence tactics, techniques, and procedures (TTPs) or standard operating procedures. Normally, a JIC responds to crisis situations by shifting its focus and assets, possibly through crisis intelligence federation, rather than by altering its organizational structure. Figure II-1 illustrates one of many possible variations of JIC organization.

(b) JICs may also be members of one or more crisis intelligence partnerships in which the JIC either receives support from extra-theater support organizations or provides support to another theater JIC. These intelligence support arrangements, known as crisis intelligence federations, may include a variety of supporting partners, including JICs, national agencies, Service intelligence organizations, and reserve units.

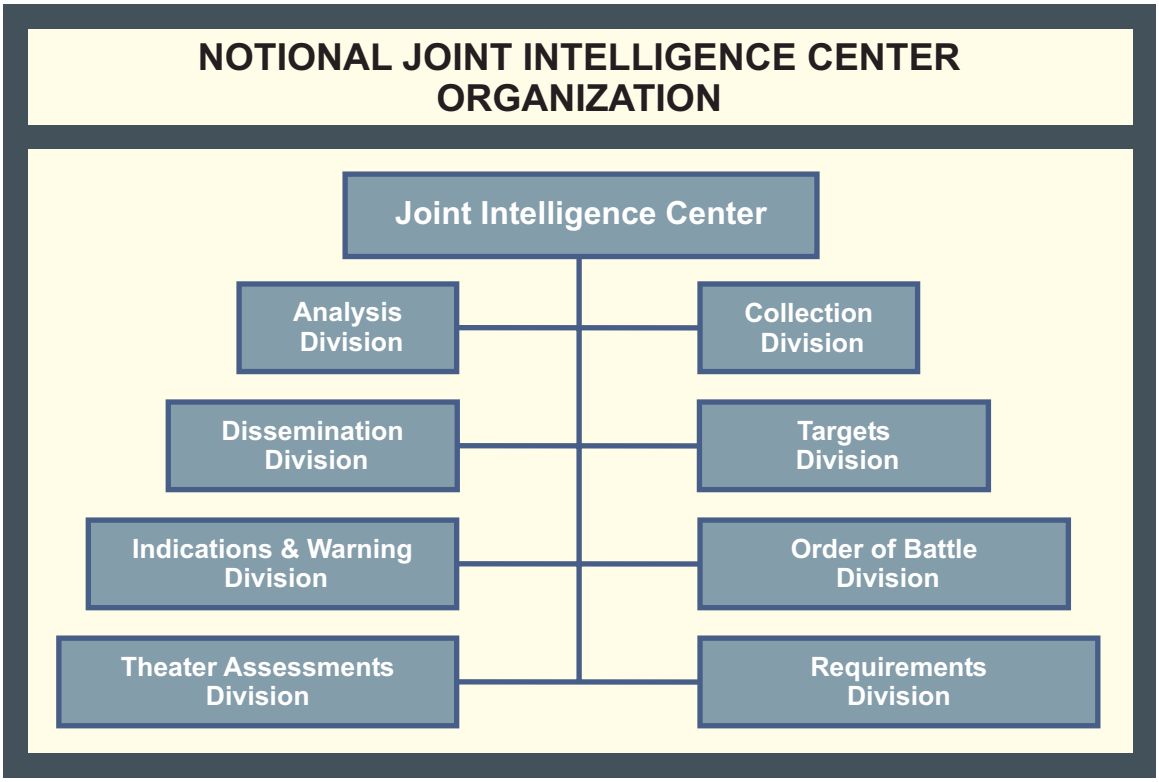


Figure II-1. Notional Joint Intelligence Center Organization

(2) **Responsibilities.** The primary responsibility of the JIC is to ensure that the intelligence needs of the combatant command and subordinate joint forces are satisfied. Other responsibilities include, but are not limited to:

(a) Maintaining and coordinating the theater collection plan and employment of theater assigned and supporting sensors.

(b) Developing and maintaining databases that support planning, operations, and targeting.

(c) Developing battle damage assessments (BDA) as required, and validating BDA from other sources.

(d) Providing continuous indications and warning (I&W) intelligence assessments.

(e) Producing JIPB products based on planning and coordination from the combatant command J-2.

(f) Providing intelligence support to, and augmenting the intelligence infrastructure of, subordinate joint forces.

(g) Providing intelligence support to other intelligence organizations as required by federated intelligence agreements and relationships.

(h) Maintaining awareness and providing amplification as required of intelligence derived threat warning events and actions.

4. Subordinate Joint Force Intelligence Organizations and Responsibilities

The organizational structure of subordinate joint force's intelligence element is determined by the JFC based on the situation and mission. All subordinate joint force J-2s, however, will at a minimum require a core element of analytical and administrative capabilities. Most situations will require augmentation of joint force intelligence capabilities through the deployment and integration of theater intelligence elements into a JISE.

a. **Subordinate Joint Force J-2.** The subordinate joint force J-2 **is responsible for planning and directing the overall intelligence effort on behalf of the JFC**. The J-2 develops and recommends PIRs based on the JFC's guidance, identifies shortfalls in intelligence capabilities and submits requests for additional augmentation, and ensures the intelligence needs of the JFC and joint force staff are satisfied in a timely manner. Additionally, at the discretion of the JFC, the J-2 provides administrative support to augmentation forces and the JISE, including personnel, information, and physical security.

Appendix A, "Joint Force J-2 Quick Reaction Checklist," contains a detailed list and generic descriptions of joint force J-2 tasks and responsibilities.

b. **Joint Force J-2 CI and Human Intelligence (HUMINT) Staff Element (J-2X).** In coordination with the theater J-2, the JFC normally establishes a J-2X. This concept is designed to integrate HUMINT and CI by combining the HUMINT operations cell (HOC) with the task force counterintelligence coordinating authority (TFCICA), both of which comprise the J-2X. The J-2X may also include a support element to provide report and source administration, linguistic services, and polygraph support. A J-2X is the HUMINT and CI focal point for the JFC. As the JFC's tasking authority for HUMINT and CI collection, the J-2X is responsible for the management, coordination, and deconfliction of HUMINT and CI collection within the operational area. The J-2X monitors and supports the activities of the joint exploitation centers (see Appendix G, "Joint Exploitation Centers"), maintains the command source registry, deconflicts source matters, and performs liaison functions with external organizations. It is imperative that a secure communications/systems architecture be established for the J-2X that is compatible with component HUMINT elements and other intelligence organizations. The J-2X should be located in a sensitive compartmented information facility (SCIF).

Additional information on the J-2X organization and responsibilities can be found in JP 2-01.2, Joint Doctrine, Tactics, Techniques, and Procedures for Counterintelligence Support to Operations.

c. **Joint Intelligence Support Element.** The subordinate joint force is usually augmented with theater intelligence production resources, which are organized into a JISE under the

supervision of the joint force J-2. **Capabilities of the JISE include order of battle (OB) analysis, identification of adversary COGs, analysis of adversary command, control, communications, and computers (C4), targeting support, collection management, and maintenance of a 24-hour watch.**

d. An example of a possible subordinate joint force J-2 organizational support package is shown in Figure II-2. This hypothetical structure should only be used as a point of departure when planning and organizing a subordinate joint force JISE. The nature and magnitude of the crisis will dictate the actual size and configuration of the JISE.

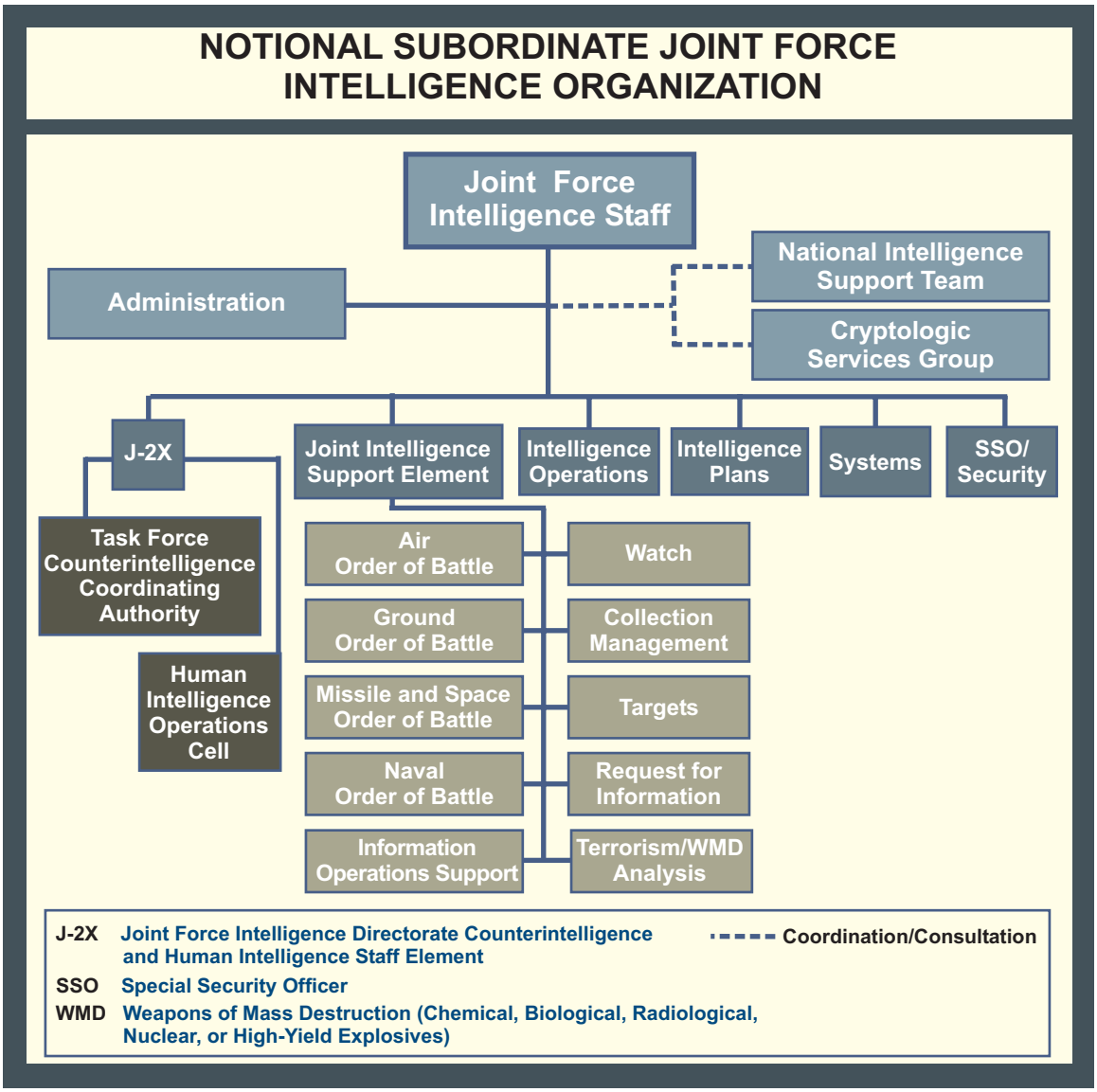


Figure II-2. Notional Subordinate Joint Force Intelligence Organization

SECTION B. NATIONAL INTELLIGENCE

5. Introduction

a. **National intelligence organizations conduct extensive collection, processing, analysis, and dissemination activities.** These intelligence organizations employ specialized resources and dedicated personnel to gain information about potential adversaries, events, and other worldwide intelligence requirements. The national intelligence organizations routinely provide support to the JFC while continuing to support national decision makers. However, **the focus of these national organizations is not evenly split among intelligence customers and varies according to the situation and competing requirements.** The joint force J-2 should take advantage of the extensive capabilities provided by these organizations.

b. Successful national support to JFCs depends upon efficient and effective cooperation and interoperability both vertically (among national and subordinate echelons) and horizontally (among national organizations). Each agency is assigned clearly defined functions and areas of concern to minimize confusion over functional responsibilities and to avoid duplication of effort.

6. National Intelligence Community Organizations and Responsibilities

The Intelligence Community (IC) refers in the aggregate to those Executive Branch agencies and organizations that are funded in the National Foreign Intelligence Program (NFIP) (see Figure II-3). The IC consists of 15 member organizations:

a. **Defense Intelligence Agency.** DIA has oversight of the Department of Defense Intelligence Production Program (DODIPP), under which all-source intelligence is produced for use by both policymakers and commanders. Under DODIPP, DIA's Armed Forces Medical Intelligence Center (AFMIC) is assigned responsibility for medical intelligence and DIA's Missile and Space Intelligence Center (MSIC) is responsible for missile and space intelligence. Additionally, DIAs Defense HUMINT Service (DHS) provides a full range of HUMINT and HUMINT-related intelligence collection services to combatant commanders and other DOD and national-level consumers. DIA also provides intelligence support in areas such as: counterintelligence, counterterrorism, counterdrug operations, computer network operations, personnel recovery, proliferation of WMD and the means of delivery, United Nations (UN) peacekeeping and coalition support, measurement and signature intelligence (MASINT), noncombatant evacuation efforts, I&W, targeting, BDA, current intelligence, collection management, intelligence architecture and systems support, and document and media exploitation capability.

b. **National Security Agency (NSA)/Central Security Service (CSS).** NSA/CSS is a unified organization structured to provide for the signals intelligence (SIGINT) mission of the United States and to ensure the protection of national security systems for all departments and agencies of the United States Government (USG).

Figure II-3. Intelligence Community Membership

c. **National Geospatial-Intelligence Agency (NGA).** NGA provides timely, relevant, and accurate geospatial intelligence (GEOINT) support to include imagery intelligence, geospatial information, national imagery collection management, commercial imagery, imagery-derived MASINT, and some meteorological and oceanographic (METOC) data and information. NGA creates tailored, customer-specific, geospatial and METOC intelligence, analytic services, and solutions to support USG activities across the range of military operations.

d. **National Reconnaissance Office (NRO).** NRO is responsible for integrating unique and innovative space-based reconnaissance technologies, and the engineering, development, acquisition and operation of space reconnaissance systems and related intelligence activities. NRO activities provide support to I&W, monitoring arms control agreements, and the planning and execution of military operations.

e. **Service Intelligence Organizations.** The Chiefs of the Military Services provide intelligence support for Departmental missions related to military systems, equipment, training, and national intelligence activities. The Services also provide support to DOD entities, including combatant commands and their components.

(1) **Army Intelligence.** The Army Deputy Chief of Staff for Intelligence (G-2) exercises staff supervision over the US Army Intelligence and Security Command (INSCOM). INSCOM provides intelligence support to strategic- and operational-level commanders in the areas of imagery intelligence (IMINT), MASINT, SIGINT, tactical HUMINT, CI, IO, and general military and scientific and technical intelligence. INSCOM elements include the National Ground Intelligence Center (NGIC), which produces multi-source intelligence products, and the 902nd Military Intelligence (MI) Brigade, which performs the CI function for the Army. G-2 is responsible for policy formulation, planning, programming, budgeting, management, staff supervision, evaluation, and oversight of intelligence, weather, and geospatial activities for the Department of the Army. G-2 has Army Staff responsibility for overall coordination of the intelligence disciplines listed above.

(2) **Air Force Intelligence.** The Air Force Director of Intelligence, Surveillance, and Reconnaissance (AF/XOI) is responsible for intelligence policy, planning, programming, evaluation and resource allocation. Other Air Force intelligence organizations include the Air Intelligence Agency (AIA) and its National Air and Space Intelligence Center (NASIC), which produces multi-source intelligence products pertaining to foreign air and space threats; Air Force Information Warfare Center (AFIWC), which provides IO-related intelligence to operational forces; and the Air Force Office of Special Investigations (AFOSI), which provides a full range of CI services.

(3) **Navy Intelligence.** The Director of Naval Intelligence (DNI) exercises staff supervision over the Office of Naval Intelligence (ONI), which provides the intelligence necessary to plan, build, train, equip, and maintain US maritime forces. The National Maritime Intelligence Center (NMIC) consists of ONI, a detachment of the Marine Corps Intelligence Activity (MCIA), the US Coast Guard (USCG) Intelligence Coordination Center, and the Naval Information Warfare Activity (NIWA). The Commander, Naval Security Group is the US Navy Service cryptologic element (SCE). The Naval Criminal Investigative Service (NCIS) provides CI services and intelligence on terrorist and unconventional warfare (UW) threats.

(4) **Marine Corps Intelligence.** The Director of Intelligence is the Commandant's principal intelligence staff officer and the functional manager for intelligence, counterintelligence, and cryptologic material. As the Service Intelligence Chief, he allocates resources and manpower to the operating forces with specific expertise in the areas of human and technical reconnaissance and surveillance, general military intelligence, human-source intelligence, CI, IMINT, SIGINT, and tactical exploitation of national capabilities (TENCAP). The Director of Intelligence exercises supervision over the MCIA. MCIA has the mission of providing tailored intelligence support to the Marine Corps operating forces with contingency planning and other requirements for intelligence products not satisfied by other theater or national assets.

f. **Central Intelligence Agency (CIA).** CIA's primary areas of expertise are in HUMINT collection, all-source analysis, and the production of political and economic intelligence.

g. **Department of State (DOS).** The State Department Bureau of Intelligence and Research (INR) performs intelligence analysis and produces studies on a wide range of political and economic topics essential to foreign policy determination and execution.

h. **Federal Bureau of Investigation (FBI).** The FBI has primary responsibility for CI and counterterrorism operations conducted in the United States. FBI CI operations overseas are coordinated with the CIA. The FBI shares law enforcement/CI information with appropriate DOD entities and combatant commands.

i. **Department of Treasury.** The Treasury Department analyzes foreign intelligence related to US economic policy and participates with the DOS in the overt collection of general foreign economic information.

j. **Department of Energy (DOE).** DOE analyzes foreign information relevant to US energy policies and nonproliferation issues.

k. **Department of Homeland Security.** The Department of Homeland Security's Directorate for Information Analysis and Infrastructure Protection analyzes the vulnerabilities of US critical infrastructure, assesses the scope of terrorist threats to the US homeland, and provides input to the Homeland Security Advisory System.

l. **United States Coast Guard.** The USCG, a component of the Department of Homeland Security, operates as both an armed force and a law enforcement organization. The USCG's Maritime Intelligence Fusion Centers Atlantic and Pacific operate under the direction of the Assistant Commandant for Intelligence and serve as the central hub for collection, fusion, analysis and dissemination of maritime intelligence and information to Coast Guard operating units, Department of Homeland Security and all members of the IC including DOD and key decision makers at the national level.

Appendix B, "National Intelligence," contains more detailed information regarding the organization, capabilities, and responsibilities of IC members.

7. National Intelligence Support Mechanisms

a. **National Agency Combatant Command Representatives. CIA, DIA, NSA, NGA, and NRO support the combatant commanders on a full-time basis through representatives.** Some of these representatives are located full-time at the command headquarters (HQ). These representatives serve as the combatant commander's advisors on how to best employ their organization's capabilities and provide liaison with their parent organizations. The combatant commander and J-2 should fully utilize these representatives to ensure that the command is familiar with the current responsibilities, capabilities, and operations of the representative's parent organization.

(1) **Director of Central Intelligence (DCI) Representative.** The DCI has assigned representatives to each of the combatant commands to coordinate CIA and other IC support to

the command, and to facilitate access to CIA resources. DCI representatives can also advise and assist the command regarding the secondary and follow-on dissemination of originator-controlled material and HUMINT Control System information IAW Director of Central Intelligence Directive (DCID) 1/7.

(2) **Defense Intelligence Support Office (DISO). DIA maintains DISOs at each of the combatant commands, US Forces Korea, and Supreme HQ Allied Powers Europe and North Atlantic Treaty Organization (NATO) HQ**. Each DISO includes a senior DIA intelligence officer, who serves as chief of the DISO and as the personal representative of the DIA Director; an administrative assistant; and a varying number of DIA functional intelligence specialists based on the needs of the supported command. The typical DISO includes a HUMINT support element (HSE), consisting of one or more DHS personnel; an intelligence production liaison officer; and a measurement and signatures intelligence liaison officer (MASLO). Some DISOs also have IT and Joint Intelligence Task Force Combating Terrorism (JITF-CT) representatives. The DISO organization enhances and expedites the exchange of information between DIA and the supported command. The DISO provides an on-site interface between DIA and the command, advising the command on the roles, missions and capabilities of DIA, while ensuring that command requirements are understood by DIA.

(3) **Defense Intelligence Agency Directorate for MASINT and Technical Collection (DIA/DT).** DIA/DT provides MASINT representatives to the combatant commands in the form of MASLOs. The MASLO helps expedite a broad spectrum of MASINT operational support between DIA/DT and the supported command. For example, the MASLO provides technical assistance on MASINT capabilities available to support military operations. Additionally, they are the means for providing feedback on the commander's operational needs for integration into MASINT-related current operations and future acquisition requirements.

(4) **NSA/CSS Representatives.** NSA/CSS provides representatives to the combatant commands in the form of **NSA/CSS representatives (NCRs)** and **cryptologic services groups (CSGs)**.

(a) **NCRs** are senior representatives of the Director, NSA, accredited to the combatant commands, other senior military commands, and the Department of State and Department of Defense. The NCRs at the military commands are the senior cryptologic authorities in the region and are the special advisors to the combatant commander for all cryptologic matters.

(b) **CSGs** are extensions of the National Security Operations Center (NSOC) and are the primary mechanism for the supported organization to gain entrance into and support from the US Cryptologic System (USCS). CSGs provide cryptologic interpretation, advice, and assistance. They advise organizations of USCS capabilities and limitations that might affect its cryptologic requirements and recommend to NSA/CSS those actions to ensure cryptologic responsiveness to the supported command.

(5) **NGA Representatives.** NGA provides representatives to the combatant commands in the form of NGA support teams (NSTs) composed of staff officers and imagery and geospatial analysts. The NST is the central point of contact (POC) for all operational and training support

from NGA. In addition, the NST helps combatant commands understand emerging GEOINT concepts, technologies and procedures, and arranges METOC support from the Joint METOC Officer.

(6) **NRO Representatives.** NRO provides representatives to the combatant commands in the form of liaison officers (LNOs) and theater support representatives (TSRs). These NRO representatives provide technical assistance relating to the capabilities of NRO systems to support operations. These LNOs/TSRs also provide insights on warfighter operational needs for integration into NRO present operations and future acquisitions.

b. **National Intelligence Support Teams. The NIST mission is to provide national level, all-source intelligence support from throughout the IC to deployed commanders during crisis or contingency operations.** NISTs are comprised of intelligence and communications experts from DIA, CIA, NGA, NSA, and other agencies as required to support the specific needs of the JFC. The Joint Staff J-2 is the NIST program's executive agent and has delegated the NIST mission to the Deputy Directorate for Crisis Operations (J-2O). J-2O manages daily operations and interagency coordination for all NISTs.

(1) **Deployment Policy.** A NIST is designed to support intelligence operations at the joint task force (JTF), component command, and/or combatant command level and is traditionally collocated with the supported/requesting command's established J-2 element. Each NIST deployment is unique based on mission, duration, team composition, and capabilities, as required. The combatant command J-2 must validate all NIST requirements identified by component commands/JTFs, and forward an official NIST request message to Joint Staff J-2O. This NIST request message begins the coordination process between the Joint Staff J-2O, the appropriate intelligence community agencies, and the requesting command. Upon Joint Staff J-2O validation of the NIST request, the requesting command (combatant command level) must ensure the NIST requirement is included in the request for forces that is subsequently sent to the Director of the Joint Staff via record message traffic. See paragraph 8b of this chapter for further information on National Intelligence coordination/requests.

(2) **Participants.** The Joint Staff J-2O manages the NIST program, to include personnel qualification, training, deployment, and administrative support while deployed and through redeployment. The program is designed to train and prepare volunteers for deployment in the event a crisis emerges.

(3) **Team Composition and Size.** The Joint Staff J-2 selects the NIST team chief from nominations submitted by participating agencies. Team composition is tailored to ensure it meets the needs of the JFC and to eliminate duplication of skills and functions. Throughout its tenure, the size and composition of the team will be reviewed and modifications will be made in coordination with the supported commander.

(4) **Required Command Support.** A NIST is not self sufficient; it requires infrastructure, transportation, logistic, and bandwidth support from the supported command.

(a) **Infrastructure.** At a minimum, a NIST requires electric power, adequate workspace within a sensitive compartmented information facility (SCIF), and "expendable"

administrative supply items.

(b) **Transportation.** The supported command must provide transportation for personnel and equipment from the continental United States (CONUS) marshalling area to the operational area during initial deployment and redeployment. The NIST is responsible for transportation from the Washington, DC area to the marshalling area. Vehicle lift from the airhead may be required dependent on the equipment and communications package deployed. If vehicles are deployed, the supported command provides required fuel and maintenance.

(c) **Logistics.** Lodging and dining facilities are provided and funded by the supported command. Additionally, the supported command will provide mission specific military equipment.

(d) **Communications Support.** The NIST is designed to provide a full range of intelligence support to a JFC, from a single agency element with limited ultra high frequency (UHF) voice connectivity to a fully equipped team with joint deployable intelligence support system (JDISS) and Joint Worldwide Intelligence Communications System (JWICS) video teleconferencing (VTC) capabilities. The supported command must provide the NIST with dedicated communications paths (i.e., bandwidth) sufficient to meet the demands of the scale of operations and requested support. Military elements are responsible for identifying the frequency requirements for spectrum-dependent equipment through the component commands to the supported combatant command's command, control, communications, and computer systems directorate (J-6) for host-nation coordination. Without advance spectrum-use planning, interference among users and a shortage of assignable frequencies may limit operations. The systems that each NIST element is capable of deploying are discussed in greater detail in Appendix B, "National Intelligence," Annex C, " Intelligence Systems in Support of Crisis Operations."

(5) **NIST and Joint Force Relationship.** The NIST is deployed in direct support of the JFC, under the staff supervision of the J-2, and will perform functions as so designated. Subject to restrictions based on security clearance and program access, all intelligence generated by the NIST is available to the J-2 organization and JFC.

(a) **NIST members will not serve as a substitute for normal military intelligence staffing nor as substitutes for augmentation.** The NIST chief is responsible for the general employment of the NIST. The element leaders are primarily involved in the intelligence liaison and agency representation.

(b) The NIST chief will ensure that only time-sensitive RFIs are directly transmitted to the NMJIC RFI Desk and that the command's intelligence center (JIC and/or JAC) is kept informed simultaneously through the COLISEUM RFI management system.

c. **Crisis Intelligence Federation.** During crises, joint forces may also garner support from the IC through the crisis intelligence federation process. **Federation identifies in-theater intelligence functions which can be accomplished by intelligence and appropriate nonintelligence DOD**

organizations operating from their home stations. Crisis intelligence federation arrangements should be preplanned and formalized in appropriate operation plans (OPLANs), OPLANs in concept format (CONPLANs), or functional plans. In situations not covered by an OPLAN, CONPLAN, or functional plan, intelligence federations should be formalized in a memorandum of agreement (MOA) or memorandum of understanding among federation partners. However, in some unanticipated situations, intelligence federations may be established quickly on an ad hoc basis. The supported combatant command J-2 is responsible for requesting, via the Joint Staff J-2, crisis intelligence federation support. Specific planning guidance for crisis intelligence federation is discussed in Chapter III, "Intelligence Operations," Section A, "Planning and Direction."

d. **Quick Reaction Teams and Other Sources of National Augmentation.** Several sources of intelligence-related augmentation are available to support a joint force during crises and contingencies. The Joint Staff J-2O will coordinate the specialized intelligence support provided by various organizations to supported combatant commands in order to preclude redundancy with any support being provided by crisis federation partners.

(1) **USJFCOM maintains a standing QRT consisting of dedicated experts in two high demand intelligence fields: targeting intelligence and collection management.** These QRTs are available to immediately deploy from USJFCOM to a requesting combatant command to support crisis or contingency operations. Requests for augmentation by USJFCOM QRT personnel are coordinated by the Joint Staff J-2 NMJIC J-2O. QRT personnel should be integrated into the theater's intelligence structure to provide enhanced targeting and collection management support.

(2) **NGA and DIA provide augmentation support to the joint force** in the form of subject matter experts or functional analysts as well as facilitating the deployment of sensors capable of providing specialized geospatial intelligence or MASINT support. These capabilities may deploy with a NIST or other joint force units, as requested.

(3) **NSA's Special Support Activity provides two-man special support teams (SSTs) for crisis response missions.** The SST provides enhanced battlespace awareness, threat warning, personnel recovery support, and tailored intelligence products as required. During the initial stabilization stages of crisis or sensitive/special operations, a combatant commander can request the immediate deployment of an SST to provide remote, limited access to NSA threat warning and intelligence networks. To further expedite augmentation during time-sensitive planning, SST notification procedures for activation and deployment of an SST can be predetermined by a MOA between NSA and the supported command. Upon request/notification, an SST can be deployed within four hours or as required by the requesting command. The team is self-sustaining for up to three days, requires logistic and transportation support, and usually redeploys after arrival of a NIST or other augmentation.

(4) Other sources of augmentation support include LNOs from the Joint Warfare Analysis Center (JWAC) and Defense Threat Reduction Agency (DTRA), combat support teams from US Strategic Command's (USSTRATCOM's) Joint Information Operations Center (JIOC), and teams of subject matter experts from USSTRATCOM headquarters.

(5) These augmentation elements are capable of providing the types of support indicated in Figure II-4. Although these augmentation elements may not fall under the staff supervision of the joint force J-2, the J-2 should nevertheless be aware of, and actively liaison with such augmentation teams on all intelligence-related matters.

e. **The Joint Staff J-2 National Military Joint Intelligence Center.** To accomplish its assigned crisis intelligence functions, the Joint Staff J-2 operates the NMJIC Alert Center, which is collocated in the Pentagon with the National Military Command Center (NMCC), Defense Collection Coordination Center (DCCC), and MASINT Operations Coordination Center (MOCC) (see Figure II-5). **The NMJIC is the focal point for all defense intelligence activities in support of joint operations.** The NMJIC is comprised of regional analysts, target analysts, operational specialists, terrorism analysts, warning intelligence officers, and collection managers from the Joint Staff J-2. Additionally, DIA has two elements collocated with the NMJIC: DCCC and the MASINT Operations Coordination Center (MOCC). Additionally, elements of NGA, CIA, NSA, representatives of the Services and, as required, other federal agencies are integral components of the NMJIC.

(1) **NMJIC Responsibilities.** The mission of the NMJIC is to provide defense intelligence support and the earliest possible warning on developing situations which may threaten US interests for the Office of the Secretary of Defense (OSD), Chairman of the Joint Chiefs of Staff (CJCS), Joint Staff, combatant commanders (through their JIC or equivalent), and Military Service secretaries and chiefs during peace, crisis, and war. It is the permanent DOD Crisis Intelligence and I&W Center. The NMJIC orchestrates the responsiveness of all national sensors and collection assets to ensure complete, mutually supportive target coverage and immediate reporting of events. It supports the combatant commands and their subordinate joint forces in exercising their wartime missions and maintains an operational link with deployed NISTs to facilitate national support during crises. As the DOD focal point for crisis intelligence, the NMJIC draws upon its centralized "all-Service, all-agency, all-source" resources and capabilities. Moreover, the NMJIC is recognized as the national focus for military intelligence issues for the entire IC, with particular emphasis on crisis management and operations. The mission of the NMJIC includes providing intelligence support to selected multinational organizations in situations where there is an imminent threat to the life and safety of multinational personnel worldwide, and in other prescribed situations as directed by appropriate authority. The NMJIC is also the focal point within the IC for military intelligence support to selected peacekeeping and humanitarian operations, and to civilian agencies involved in emergency and disaster relief operations.

(2) **NMJIC Alert Center.** Deputy Directorate for Crisis Management (J-2M) provides direct analytical and intelligence support to the NMCC through the NMJIC Alert Center, a 24-hour all-source, multi-discipline intelligence center which monitors and reports on current and emerging crisis situations. The NMJIC Alert Center also **validates and provides positive control and direct management of crisis-related and time-sensitive RFIs** (response required within 24 hours) requiring national-level intelligence products in support of commanders, planners, and other decision makers. The Alert Center assigns requirements to the appropriate national

NATIONAL AUGMENTATION SUPPORT

Team/Element	Mission	Origination	Deployment Method	Number & Composition	Location/Integration Requirements	Duration and Redeployment
USJFCOM Quick Reaction Team (QRT)	LD/HD Skill Set Direct Target Support Through Entire Targeting Cycle	Unified Command J-2: Intel	CJCS WARNORD & Combatant Commander Request	4-8 Designated SMEs	Dedicated QRT at USJFCOM; Train & Exercise w/Theaters; Augment/ Integrate Into Theater Ops	Not to Exceed 180 Days & Redeploy Upon Steady State or First Combat Unit Redeployment
National Intelligence Support Team (NIST)	All-Source Intelligence Analysis Support	DOD Agency Lead;CIA: Intel	Combatant Commander Request & CJCS DEPORD	1-20 National IC Representatives	NCR/Deploy to Support Theater Intelligence Ops	Not to Exceed 90 Days; Replaced with theater assets as crisis matures into sustained operations
Joint Warfare Analysis Center (JWAC) Liaison Officers	Reach-back for Infrastructure Target System & Critical Node Development	Unified Command J-3: No Intel	Combatant Commander Request & CJCS DEPORD	1-3 Designated SMEs	At JWAC; Deploy for Exercises, Crisis/Combat	Duration of the Conflict & Redeploy Upon Combatant Commander Release
Defense Threat Reduction Agency (DTRA) Liaison Officers	WMD Target Development and Consequence Mgmt.	DOD Agency: Possible Intel	Combatant Commander Request & CJCS DEPORD	2-4 Designated SMEs	At DTRA; Deploy for Exercises, Crisis/Combat	Duration of the Conflict & Redeploy Upon Combatant Commander Release
Joint Information Operations Center (JIOC) Customer Service Team	Information Operations Planning and Execution Support	Unified Command J-3: Some Intel	Combatant Commander Request & CJCS DEPORD	# Contingency Dependent; Designated SMEs	JIOC/ACC (AIA) Deploy for Exercises, Crisis/Combat	Duration of the Conflict & Redeploy Upon Combatant Commander Release
National Geospatial-Intelligence Agency (NGA)	Geospatial Intelligence Support	DOD Agency: Intel	Combatant Commander Request & CJCS DEPORD	Up to 8 Designated SMEs	At NGA; Deploy for Exercises, Crisis/Combat	Duration of the Conflict & Redeploy Upon Combatant Commander Release

Figure II-4. National Augmentation Support

NATIONAL AUGMENTATION SUPPORT (cont'd)

Team/Element	Mission	Origination	Deployment Method	Number & Composition	Location/Integration Requirements	Duration and Redeployment
USSTRATCOM Joint Space Support Team	Operational Support to Maximize Space-Based Assets	Unified Command J-3: One Intel	Combatant Commander Request & CJCS DEPORD	Up to 8 Designated SMEs	At USSTRATCOM; Deploy for Exercises, Crisis/Combat	Duration of the Conflict & Redeploy Upon Combatant Commander Release
USSTRATCOM Theater Planning Response Cell	Reach-back for Nuclear Tgt. Development, Weaponeering, DGZ Const., Nominal, & Consequence Mgmt.	Unified Command J-5: Possible Intel	Combatant Commander Request or Appropriate NUC WARNORD	1-2 Designated SMEs	At USSTRATCOM; Deploy for Exercises, Crisis/Combat	Duration of Nuclear Planning & Redeploy Upon Combatant Commander Release
DIA/Directorate for MASINT and Technical Collection	MASINT Support	DOD Agency: Intel	Combatant Commander Request & CJCS DEPORD	1-2 Designated SMEs	NCR; Deploy for Exercises, Crisis/Combat	Duration of the Conflict & Redeploy Upon Combatant Commander Release
DIA/Defense HUMINT Service	HUMINT Support	DOD Agency: Intel	Combatant Commander Request & CJCS DEPORD	As Required	NCR; Deploy for Exercises, Contingencies	Duration of the Conflict & Redeploy Upon Combatant Commander Release
National Security Agency (NSA) Space Support Team	Access to NSA threat warning & intelligence networks during crisis/sensitive operations	DOD Agency: Intel	Combatant Commander Request or Notification as per MOA between Command and NSA	2 Designated SMEs	At NSA Dedicated 90-day Alert Status; Movement Upon 4-hour Notification; Deploy for Crisis/Combat	Not to Exceed 30 days; Redeploy Upon Steady State or Arrival of NIST and/or Follow-on Augmentation

LEGEND

AIA	Air Intelligence Agency	IC	Intelligence Community	SME	subject matter expert
CIA	Central Intelligence Agency	J-2	Intelligence Directorate of a Joint Staff	USJFCOM	United States Joint Forces Command
CJCS	Chairman of the Joint Chiefs of Staff	J-3	Operations Directorate of a Joint Staff	USSTRATCOM	United States Strategic Command
DEPORD	deployment order	J-5	Plans Directorate of a Joint Staff	WARNORD	warning order
DGZ	designated ground zero	LD	low density	WMD	weapons of mass destruction
DHS	Defense HUMINT Service	MASINT	measurement and signature intelligence		
DIA	Defense Intelligence Agency	MOA	memorandum of agreement		
HD	high demand	NCR	national cryptologic representative		
HUMINT	human intelligence	NUC	nuclear		

Figure II-4. National Augmentation Support (cont'd)

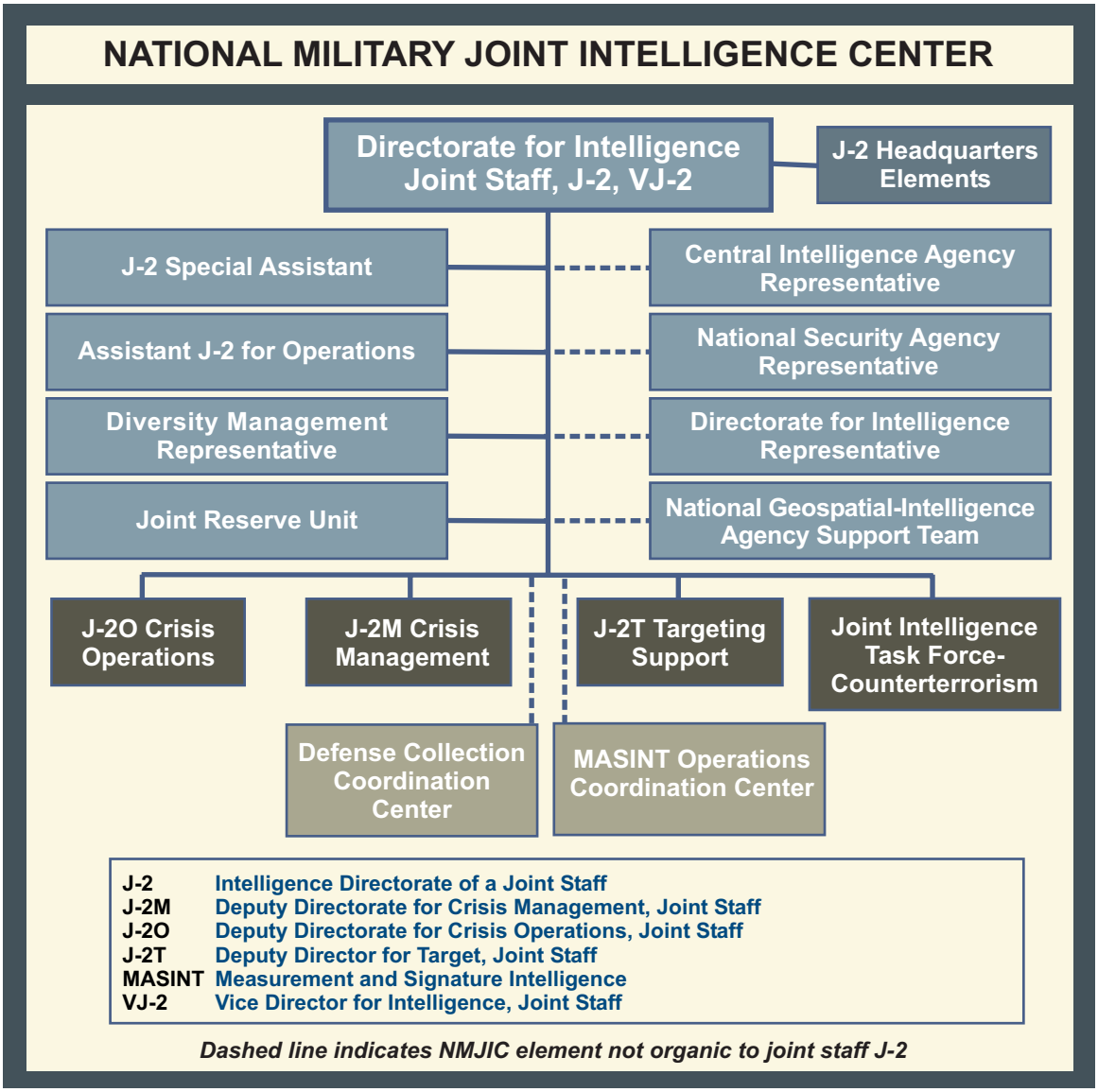


Figure II-5. National Military Joint Intelligence Center

producer IAW the DODIPP and/or direct coordination and ensures that products and responses are timely and satisfy the requester's needs. RFIs should be submitted to the NMJIC through COLISEUM. If a developing situation escalates into a crisis, the relevant Alert Center regional desk officer is augmented with analytical support, or an intelligence cell, intelligence working group (IWG), or intelligence task force (ITF) is formed. Thus, support may range from one additional analyst in an intelligence cell to a 24-hour IWG or ITF.

(a) **Intelligence Cell.** A cell is established upon indications that a threat to US interests or personnel may exist or in other potential emergency situations. The cell is responsible for monitoring and providing a continuous assessment of the developing situation. An intelligence cell is generally formed with personnel organic to the NMJIC and operates on extended duty hours. However, 24-hour operations and augmentation from DIA may be warranted.

(b) **Intelligence Working Group.** As a crisis develops, an IWG may be established within the NMJIC Alert Center **to provide focused coverage of crisis requirements**. Specifically, the IWG is formed at the lowest level of response to a particular crisis situation; provides all-source intelligence on the crisis situation to the OSD, Chairman of the Joint Chiefs of Staff, Joint Staff, Services, combatant commands, and deployed operational forces; and is normally manned from J-2 and DIA with reserve augmentation.

(c) **Intelligence Task Force.** If a crisis situation continues to escalate, the Joint Staff J-2 may decide to form an ITF to provide increased capabilities for focused all-source intelligence support. **The size of the ITF depends on the severity, complexity, and duration of the crisis and may be formed using an IWG as its core.** Figure II-6 displays a basic ITF organization. NSA, NGA, CIA, the Services, and other major government organizations generally augment an existing IWG to form an ITF. **The ITF focuses intelligence resources, answers RFIs, expedites dissemination of intelligence, and provides rapid responses to special tasking.** Specifically, the ITF:

1. Is convened by the Joint Staff J-2 whenever a crisis operations team (COT) is convened by the J-3. (An ITF may be convened by the J-2 without a COT being convened if it is required to support the NMJIC.)

2. Provides time-critical responses to requirements from the OSD, Chairman of the Joint Chiefs of Staff, Joint Staff, Military Services, combatant commands, and deployed operational forces.

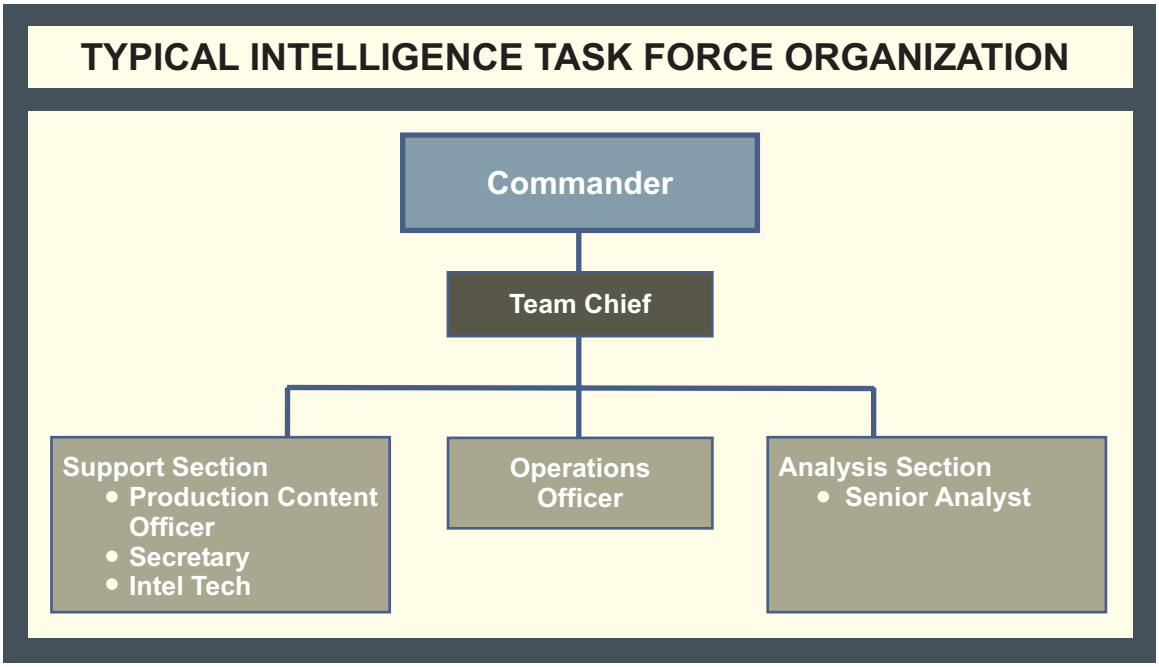


Figure II-6. Typical Intelligence Task Force Organization

3. Provides timely warning to the OSD, Chairman of the Joint Chiefs of Staff, Joint Staff, Military Services, and the combatant commands of hostilities or potential threats to US interests in the ITF's area of concern.

4. Develops and tailors an all-source intelligence collection strategy plan for the DOD response to the crisis.

5. Responds to requirements from other USG agencies responsible for crisis response activities.

6. Responds to requirements of the UN and/or foreign governments consistent with DCI guidelines, and in coordination with the DIA Foreign Disclosure Office.

7. Coordinates tasking of other USG agencies in support of the OSD, Chairman of the Joint Chiefs of Staff, combatant commanders, subordinate JFCs, and other consumers.

(3) **Crisis Operations Support.** The Joint Staff J-2O is responsible for providing intelligence operational support and augmentation to combatant commands during contingency or crisis operations.

(a) **Operational Support.** J-2O is responsible for deployment of NISTs and maintains formal relationships with CIA, NGA, and NSA, which allow J-2O to tailor mission-specific teams to meet the JFC's intelligence requirements. J-2O recruits, trains, and maintains a cadre of military and civilian personnel and systems that are prepared to deploy on short notice. It also provides NISTs for combatant command exercises. J-2O is the requirements functional manager of the JWICS and JWICS Mobile Integrated Communications System (JMICS) programs, and provides guidance on the best use for collaborative intelligence systems support to the operational commander. J-2O is also responsible for managing, adjudicating, and validating requirements for fielded, operational intelligence systems from combatant commands and national agencies.

(b) **Joint Exercise Support.** J-2O orchestrates national intelligence support to major OSD, CJCS and combatant command exercises. It provides this national intelligence support through active participation in the exercise planning and execution process. It ensures appropriate intelligence assessments, products, systems, procedures and relationships are replicated for the exercise training audience. J-2O also provides intelligence expertise in the development and execution of training and exercise scenarios for the Joint Staff continuity of operations (COOP) program.

(c) **Crisis Augmentation.** J-2O coordinates individual personnel augmentation to the combatant commands during crisis situations. It also coordinates DIA external augmentation (e.g., DIA LNOs, NIST members) and internal augmentation (e.g., NMJIC Alert Center IWGs and ITFs). It is responsible for intelligence policy guidance, deployment readiness, support, and intelligence augmentation

to the Joint Staff COOP. Additionally, J-2O is the executive agent for Crisis Intelligence Federation and provides Joint Staff oversight of QRTs.

(4) **NMJIC Targeting and Battle Damage Assessment Support.** Within the Joint Staff J-2, **the Deputy Directorate for Targets (J-2T) is the single DIA manager and point of entry for national-level target intelligence support for conventional, information, special, and technical operations to the Joint Chiefs of Staff (JCS) and combatant commands**. J-2T's missions include serving as the focal point for community-wide target intelligence support to the President, Secretary of Defense (SecDef), Chairman of the Joint Chiefs of Staff, Joint Staff, and combatant commands; coordinating national-level target intelligence support for CJCS/ combatant command deliberate and crisis action planning and ongoing operations; directing national-level BDA; and exercising overall responsibility for joint target intelligence policy, standards, procedures, requirements, and automation.

(a) The Target Operations Division (J-2T-1) focuses national efforts for conventional, IO, and special targeting. Targeting support is provided to national-level decision makers, combatant commands, and supported commands to assist in crisis response or deliberate planning efforts. This division also coordinates the efforts of the targeting community (DIA, NSA, NGA, CIA, JWAC, DTRA and JIOC experts) to ensure the best target intelligence information is distributed. J-2T-1 provides exercise and operation national-level BDA support to the combatant commands; coordinates and provides targeting community assessments to the Joint Staff J-2, Chairman of the Joint Chiefs of Staff, and OSD; and coordinates munitions effectiveness assessment and weaponeering analyses.

(b) The Target Plans Division (J-2T-2) is responsible for the development, coordination, and maintenance of joint target intelligence policy, standards, and procedures, to include target materials production programs and target automation. J-2T-2 coordinates target intelligence issues and assessments, and leverages the collective resources and capabilities of the IC to satisfy target intelligence requirements through the Secretariat of the Military Targeting Committee.

(c) When warranted by events, J-2T organizes and directs the activation and operation of the NMJIC Targeting and BDA Cell (NTBC) comprised of personnel from J-2T, NGA, DIA, the Services, and other USG agencies. The NTBC is the single national-level source of targeting and BDA support to the Joint Staff and combatant commands during contingency operations. The NTBC also supports the combatant commands by providing IC coordinated target development and analyses to combatant command J-2s and their targeting elements. When requested, the NTBC provides federated phase 1, 2, and 3 BDA support to theater and national elements. The cell may also be augmented with personnel from DIA, NSA, NGA, CIA, JWAC, DTRA and JIOC.

(5) **The Joint Intelligence Task Force — Combating Terrorism is a component of the Joint Staff J-2** and is responsible for directing collection, exploitation, analysis, and dissemination of all-source intelligence in support of DOD force protection, counterterrorism, and antiterrorism operations and planning. The JITF-CT also focuses on providing strategic and

tactical warning exposing and exploiting terrorist vulnerabilities, and supporting operations to prevent terrorists and their sponsors from acquiring increased capabilities, particularly in the area of WMD.

f. **DIA Defense Collection Coordination Center** is collocated with, and provides tasking interface and expert advice to, the NMJIC. Operating 24 hours a day, the DCCC facilitates timely and responsive management, coordination, validation, approval, and submission of all-source time-sensitive collection requirements supporting the combatant commands, Joint Staff, DIA, Military Services, and other DOD organizations. The DCCC provides direct support to the J-2 NMJIC analysts, ITFs, and IWGs. As the DOD focal point for time-sensitive collection, the DCCC serves as the information base for questions regarding time-sensitive collection issues. Specific DCCC responsibilities include:

(1) Formulating and validating time-sensitive intelligence collection and reporting requirements in coordination with the user.

(2) Managing the submission of time-sensitive collection requirements to satisfy user needs.

(3) Assigning appropriate priorities to available collection and reporting resources.

(4) Recommending reallocation and use of collection assets and resources.

(5) Monitoring satisfaction of collection requirements.

g. **MASINT Operations Coordination Center.** The MOCC, located in the NMJIC, is the entry point for coordinating quick response MASINT requirements. The MOCC facilitates timely and responsive management and coordination of MASINT time-sensitive and short duration collection requirements for the combatant commands, Joint Staff, DIA, Military Services and other DOD organizations. Non-time-sensitive requirements are handled through the MASINT Requirements System (MRS) for tasking and registry.

h. **DIA Operational Intelligence Coordination Center**, located in the Defense Intelligence Analysis Center (DIAC), serves as the crisis management office for DIA's Directorate for Analysis (DI). The OICC is the single point of contact in DI for requirements involving analytical support during crisis situations and for sustained military operations. Response times are driven by criticality, time sensitivity, and requestor priority. The OICC transitions to 24-hour operations as required, and the size and number of OICC watch teams varies depending upon the nature and duration of each crisis.

8. Procedures for Requesting National Intelligence Support

a. **National Intelligence Production Support. The JIC is the primary focal point for providing intelligence support to the combatant command.** The JIC must analyze theater intelligence production requirements, collection requirements, and RFIs from subordinate

commands to determine whether such intelligence needs can be met with organic resources or may require national-level assistance. If the JIC determines national-level production assistance is required, a formal request will be prepared in the form of an RFI. The flow of RFIs from JICs to national intelligence agencies differs only slightly from peacetime to crisis. In all situations, DIA serves as the combatant command's portal for requesting national-level intelligence production support.

(1) **Noncrisis Request Procedures.** The DIA ensures the expeditious flow of military intelligence from the national level through the JICs to deployed forces during peacetime. RFIs are forwarded from the JIC to the DIA/DI/OICC and/or production agency. If the JIC determines national-level intelligence collection is required to meet theater intelligence production requirements, a formal collection request will be prepared IAW the appropriate DIA manual (DIAM) and forwarded to DIA's Directorate for MASINT and Technical Collection (see Figure II-7).

(2) **Crisis Request Procedures.** The NMJIC is the national focal point for crisis intelligence in support of joint operations and is the single point of entry at the national level for crisis RFIs. Likewise, DIA DCCC is the focal point for the receipt and processing of time-sensitive collection requirements forwarded by the theater JICs. Additionally, deployed NISTs may serve as a direct link to the NMJIC RFI desk and DCCC when the joint force J-2 determines that time-sensitive collection requirements or RFIs require national support. For tracking purposes, the JIC or equivalent will receive a simultaneous copy of all RFIs forwarded by the NIST (see Figure II-8).

b. **National Intelligence Augmentation Support.** Combatant commands will coordinate with the Joint Staff J-2O via record message all requests for external support from NISTs, QRTs, federation, and augmentation from national intelligence agencies that involve personnel and/or equipment. All support requests, with the exception of requests for CIA support, are submitted to Joint Staff J-2O via the combatant command for validation and subsequent action. Requests for CIA personnel/equipment support should be submitted directly to CIA for action.

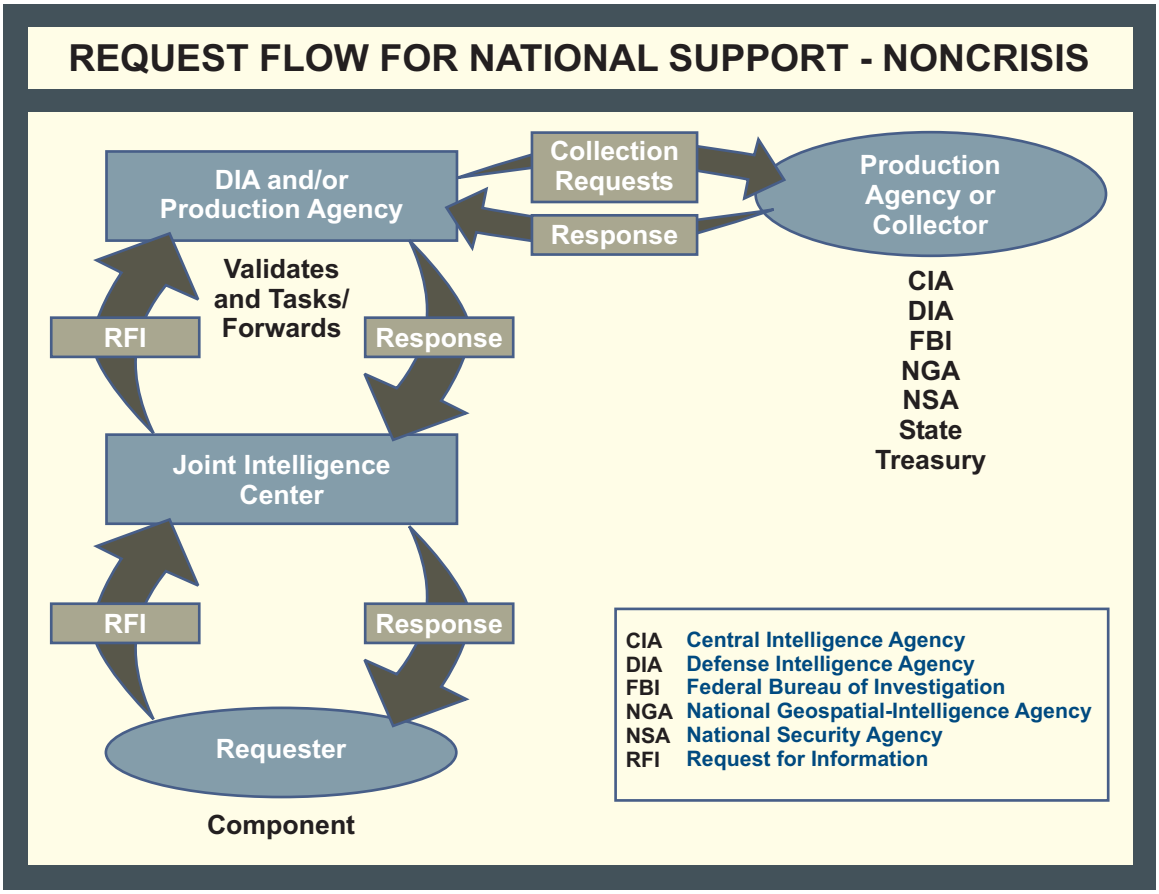


Figure II-7. Request Flow for National Support — Noncrisis

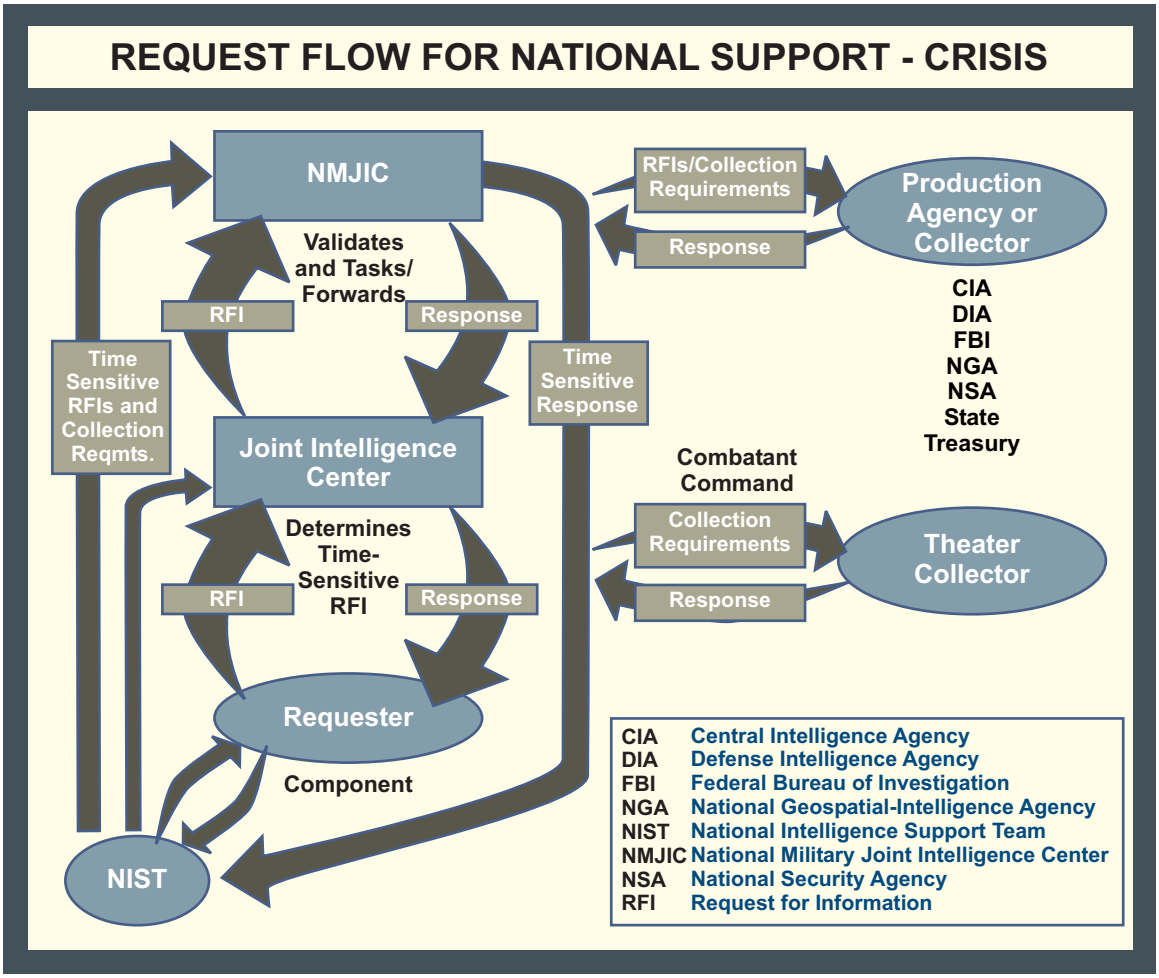


Figure II-8. Request Flow for National Support — Crisis

Intentionally Blank

CHAPTER III
INTELLIGENCE OPERATIONS

". . . that no war can be conducted successfully without early and good intelligence, and that such advices cannot be had but at very great expense."

The Duke of Marlborough
1650-1722

1. Introduction

Intelligence supports joint operations by providing critical information and finished intelligence products to the combatant command, the subordinate Service and functional component commands, and subordinate joint forces. Commanders at all levels depend on timely, accurate information and intelligence on an adversary's dispositions, strategy, tactics, intent, objectives, strengths, weaknesses, values, capabilities, and critical vulnerabilities. The intelligence process is comprised of a wide variety of interrelated intelligence operations. These intelligence operations (planning and direction, collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback) must focus on the commander's mission and concept of operations (CONOPS) (see Figure III-1).

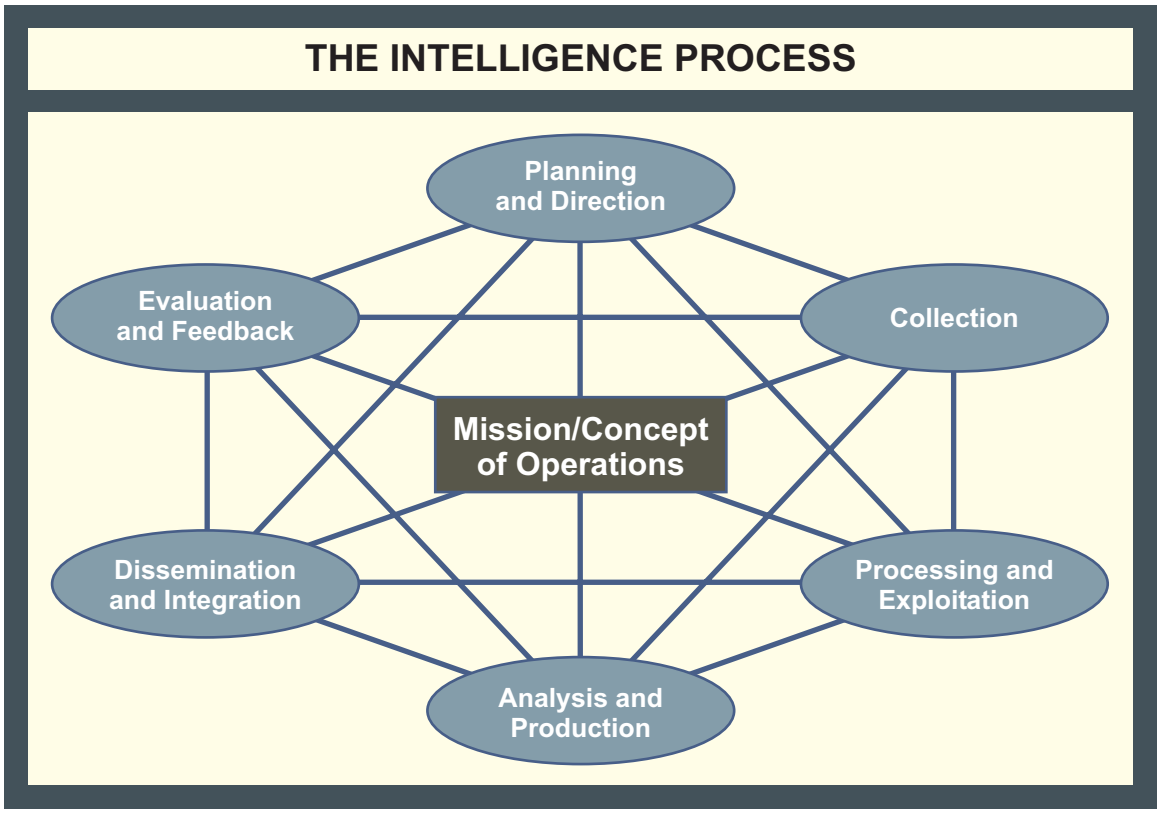


Figure III-1. The Intelligence Process

2. The Intelligence Process

The intelligence process describes how the various types of intelligence operations interact to meet the commander's intelligence needs. **The intelligence process provides a useful model that, albeit simplistic, nevertheless facilitates understanding the wide variety of intelligence operations and their interrelationships. There are no firm boundaries delineating where each operation within the modern intelligence process begins or ends.** Intelligence operations are not sequential; rather they are nearly simultaneous. For example, electronic intelligence (ELINT) data may be automatically processed and disseminated by the Distributed Common Ground/Surface System (DCGS) while simultaneously cross-cueing additional platforms for additional intelligence collection. Additionally, not all operations necessarily continue throughout the entire intelligence process. For example, during processing and exploitation, information may be disseminated directly to the user from an unmanned aerial vehicle (UAV) or other source, without first undergoing detailed all-source analysis and intelligence production. The increased tempo of military operations requires an unimpeded flow of automatically processed and exploited data that is both timely and relevant to the commander's needs. This unanalyzed combat information must be simultaneously available to both the commander (for time-critical decision making) and to the intelligence analyst (for the production of current intelligence assessments). Examples of uses for such unanalyzed combat information include, but are not limited to time-sensitive targeting, personnel recovery operations, and threat warning alerts. Likewise, the analysis, production, and dissemination of intelligence products must be accomplished in time to support the commander's decision-making needs.

a. Joint intelligence operations begin with the **identification of a need for intelligence regarding all relevant aspects of the battlespace, especially the adversary**. These intelligence needs are identified by the commander and all joint force staff elements, and are formalized by the J-2 as intelligence requirements early in the planning process. Those critical pieces of intelligence the commander must know by a particular time to plan and execute a successful mission are identified as the commander's PIRs. PIRs are identified at every level and are based on guidance obtained from the mission statement, the commander's intent, and the end state objectives.

b. **Intelligence requirements** provide the basis for current and future intelligence operations, and are prioritized based on consumer inputs during the planning and direction portion of the intelligence process. The J-2 provides the focus and direction for collection requirements to support the combatant command or subordinate joint force.

c. **The collection portion of the intelligence process** involves tasking appropriate collection assets and/or resources to acquire the data and information required to satisfy collection objectives. Collection includes the identification, coordination, and positioning of assets and/or resources to satisfy collection objectives.

d. Once the data that might satisfy the requirement is collected, it undergoes processing and exploitation. **Through processing and exploitation, the collected raw data is transformed into information** that can be readily disseminated and used by intelligence analysts to produce

multidiscipline intelligence products. Relevant, critical information should also be disseminated to the commander and joint force staff to facilitate time-sensitive decision making. Processing and exploitation time varies depending on the characteristics of specific collection assets. For example, some ISR systems accomplish processing and exploitation automatically and in near simultaneity with collection, while other collection assets, such as HUMINT teams, may require substantially more time. Processing and exploitation requirements are prioritized and synchronized with the commander's PIR.

e. **The analysis and production portion** of the intelligence process involves integrating, evaluating, analyzing, and interpreting information from single or multiple sources into a finished intelligence product. The demands of the modern battle require intelligence products that anticipate the needs of the commander and are timely, accurate, usable, complete, relevant, objective, and available.

f. **Properly formatted intelligence products are disseminated** to the requester, who integrates the intelligence into the decision-making and planning processes. In the case of threat warning alerts essential to the preservation of life and/or vital resources, such information must be immediately communicated directly to those forces, platforms, or personnel identified at risk so the appropriate responsive action can be taken once such notification has been acknowledged.

g. **Intelligence operations, activities and products are continuously evaluated.** Based on these evaluations and the resulting feedback, remedial actions should be initiated, as required, to improve the performance of intelligence operations and the overall functioning of the intelligence process.

h. The remainder of this chapter discusses each type of intelligence operation and its associated activities in detail. Organizational and staff responsibilities for executing the various types of intelligence operations are depicted in Appendix H, "Intelligence Operations Execution Responsibilities."

SECTION A. PLANNING AND DIRECTION

3. Overview

Intelligence planning and direction, while continuously conducted, normally intensifies during operation planning. However, **the most dynamic period of intelligence planning and direction occurs during the execution and assessment of ongoing operations**. JIPB helps the joint force J-2 focus and direct intelligence planning to ensure it provides a proper foundation for the entire intelligence process. Planning and directing involves the activities shown in Figure III-2.

4. Intelligence Requirements

Successful intelligence support to military operations demands that some universal principles be understood and applied. **The J-2 participates fully in the planning and decision-making**

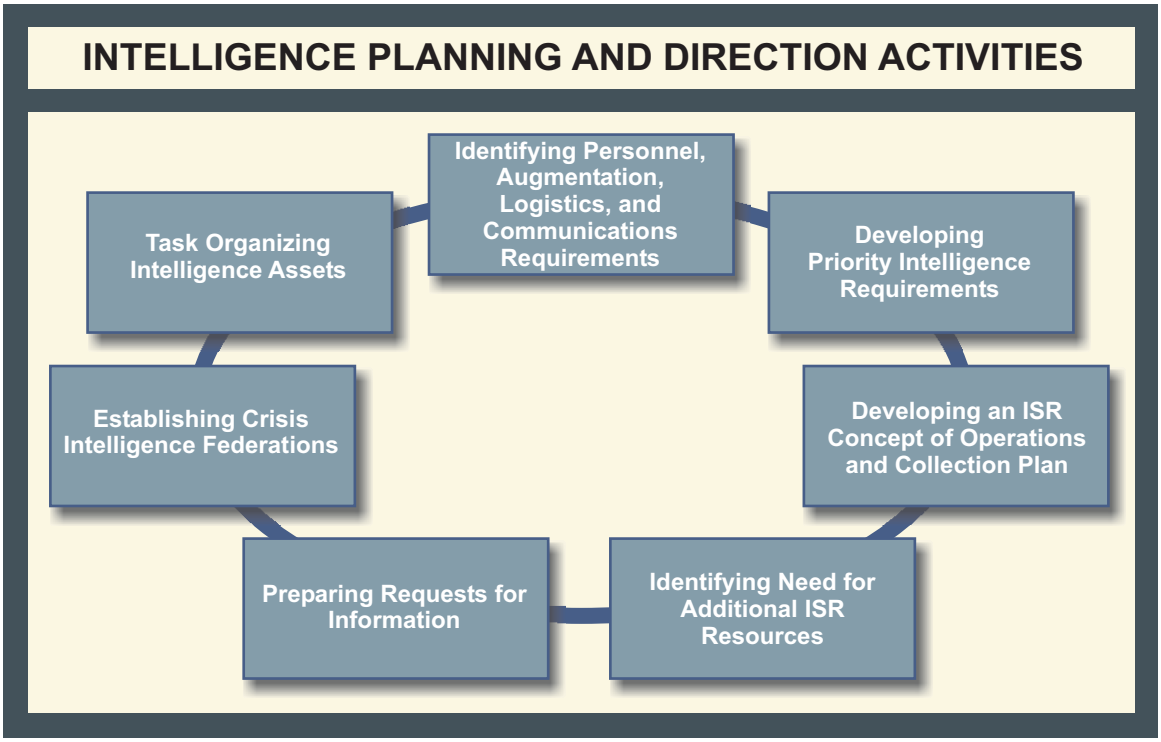


Figure III-2. Intelligence Planning and Direction Activities

process, contributing knowledge concerning the battlespace, and receiving guidance to help focus the intelligence effort. The intelligence planner examines specific operational tasks and subtasks, then determines what intelligence support and information will be required to achieve mission success.

a. Additionally, **the JFC should provide commander's critical information requirements (CCIRs) to the joint staff and components**. CCIRs comprise a comprehensive list of information requirements identified by the commander as being critical in facilitating timely information management and the decision-making process that affect successful mission accomplishment. In the course of mission analysis, the intelligence planner identifies the intelligence required to answer the CCIRs. Mission analysis leads to the development of intelligence requirements (general or specific subjects upon which there is a need for the collection of information or the production of intelligence.) **Those intelligence requirements deemed most important to mission accomplishment are identified by the commander as PIRs**. Based on the command's intelligence requirements, the intelligence staff develops more specific questions known as information requirements (those items of information that must be collected and processed to develop the intelligence required by the commander). **Those information requirements that are most critical or that would answer a PIR are known as essential elements of information (EEIs).** Figure III-3 illustrates how information requirements (including EEIs) are derived from, and are intended to answer, intelligence requirements (including PIRs).

b. The categories, types, and level of detail of intelligence requirements differ from echelon to echelon. Intelligence necessary to support the operational level might be inappropriate at the tactical

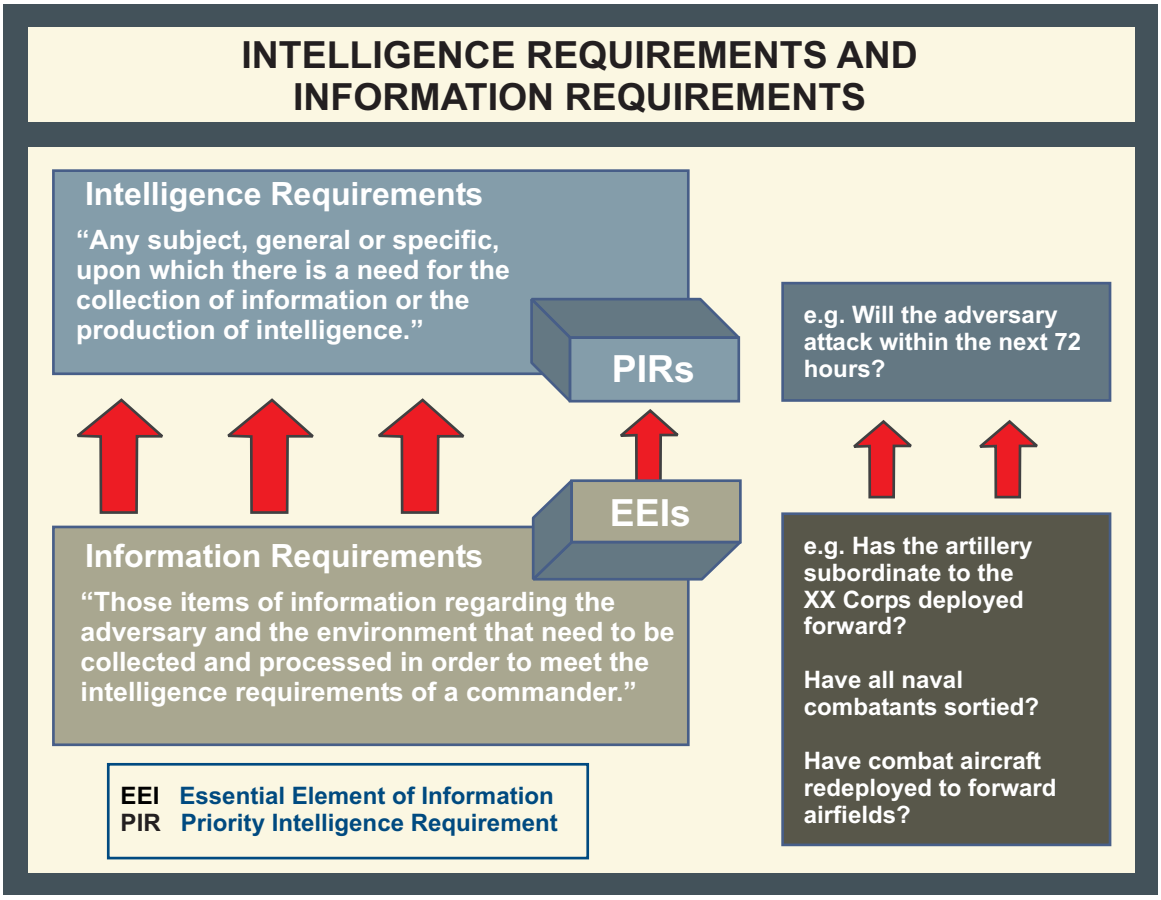


Figure III-3. Intelligence Requirements and Information Requirements

level. With some exceptions, the higher echelon commander's intelligence requirements are less detailed and much broader in scope than those of subordinate commanders. An intelligence planner who tries to use intelligence beyond what is required to support the organization may overburden the intelligence infrastructure with too much information and needlessly complicate the commander's decision-making process.

Appendix C. "Representative Intelligence Requirements," contains a generic list of sample intelligence requirements.

c. **RFIs respond to customer requirements, ranging from dissemination of existing products through the integration or tailoring of onhand information to scheduling original production.** The information must be timely, accurate, and in a usable format. The intelligence office translating the customer's requirement and the primary intelligence producer determine how best to meet the customer's needs. If it is determined that new, finished intelligence derived from original research is required to satisfy all or a portion of the RFI, then that need is expressed formally within the DODIPP as a production requirement (PR). If it is determined that insufficient information exists to answer an RFI, then a collection requirement is prepared IAW the appropriate DIA manual.

(1) Requirements that cannot be satisfied are submitted as RFIs or collection requirements to the next higher echelon. Each echelon is responsible for validating, prioritizing and, if possible, satisfying the RFI or collection requirement before forwarding it to the next level. RFIs should be satisfied at the lowest level possible. If the information required to satisfy an RFI does not exist, the requester is informed and a decision is made to initiate collection and/or production. Decisions to expend collection resources should be made at the lowest level possible.

(2) Validation, a process associated with the collection and production of intelligence, confirms that an intelligence collection or production requirement is sufficiently important to justify the dedication of intelligence resources, does not duplicate an existing requirement, and has not been previously satisfied. Information copies of the requirement should be forwarded to supporting intelligence organizations to alert potential respondents to the requirement.

5. Augmentation Requirements

The demand for intelligence increases significantly at all levels during crisis and wartime operations. Optimal use of available intelligence assets throughout the IC and combatant commands is essential to meeting these increasing customer needs. These limited intelligence

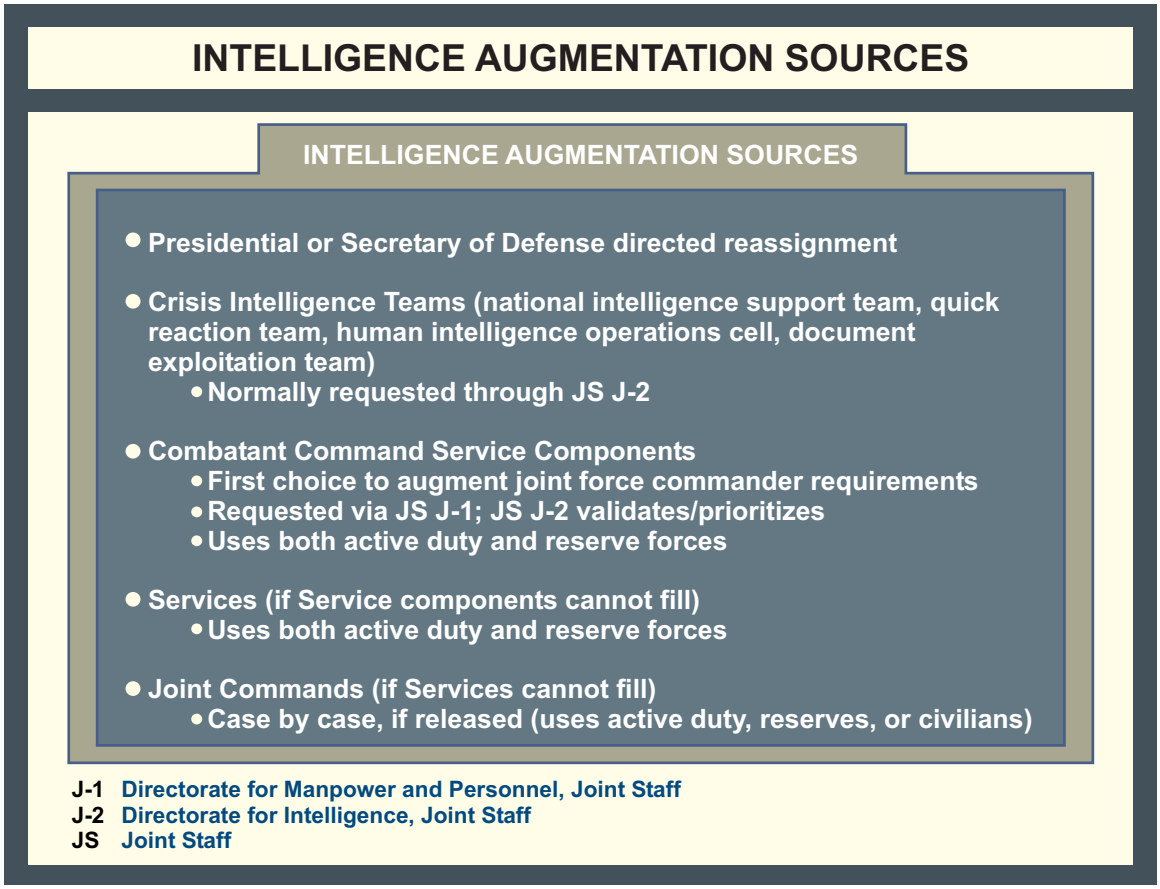


Figure III-4. Intelligence Augmentation Sources

assets can be effectively brought to bear on the crisis through the personnel augmentation process. Some potential augmentation sources for the JFC are depicted in Figure III-4.

a. **The JFC initiates augmentation by defining personnel shortfalls beyond those that can be filled through the components.** The Joint Staff takes the lead in augmenting the NMJIC intelligence staff and coordinating individual augmentation to meet the JFC's needs.

(1) Normally, active duty intelligence personnel are reassigned to support the operation on a temporary basis within-theater through established personnel management channels.

(2) At the national level, the President or Secretary of Defense can direct active duty personnel to new assignments in support of the joint force. Additionally, teams of intelligence personnel can be positioned for crisis deployment (NISTs, USJFCOM QRTs, HOCs, or other teams of intelligence personnel) upon receipt of a requirement from the supported combatant command. Each of the Services and IC agencies have established channels to deploy mission-specific intelligence teams and support personnel. Requesting commands must be prepared to logistically support these external augmentation elements.

b. Personnel augmentation requirements should be IAW Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 1301.01, *Policy and Procedures to Assign Individuals to Meet Combatant Command Mission Related Temporary Duty Requirements*, and reflected in the combatant command's joint table of mobilization and distribution (JTMD). Also, the JTMD should reflect the need for Reserve personnel, including individual mobilization augmentees, selected Reserve personnel, or individual ready Reserve personnel.

For further information regarding mobilization of reserve personnel for augmentation, refer to JP 4-05, Joint Doctrine for Mobilization Planning.

c. A combatant command may make a request to the Joint Staff J-2 for specific national intelligence agency capabilities. The J-2 will evaluate and coordinate these requirements with the J-3/Joint Strategic Plans Staff (J-5) and national intelligence agencies and tailor the composition of the deployment packages to meet those needs. The combatant command J-2 may integrate these supporting capabilities with the command's JIC and the subordinate joint force JISE. The deployment packages, including NISTs, USJFCOM QRTs, HOCs, and document exploitation (DOCEX) teams, provide access to the entire range of capabilities resident in the national intelligence agencies and can focus those capabilities on the JFC's intelligence requirements.

6. Crisis Intelligence Federation Planning Guidance

Intelligence federation enables combatant commands to form support relationships with other theater JICs, Service intelligence units, Reserve organizations, or other intelligence agencies to assist with the accomplishment of the joint force's mission. **These relationships, called federated partnerships, are formal agreements intended to provide a rapid, flexible, surge capability enabling personnel from throughout the IC to assist the combatant command with specific functional areas while remaining at their normal duty stations.** Combatant commands initiate the federation process by

assessing their intelligence shortfalls and requesting, via formal message, federated partnership support. Federated support can be provided in specific functional areas directly related to the crisis, or by assuming temporary responsibility for noncrisis-related areas within the combatant command's area of responsibility (AOR), thereby freeing the supported command's organic assets to refocus on crisis support.

a. The details of a crisis intelligence federated partnership should, if possible, be coordinated and agreed upon by the supported combatant command J-2, the Joint Staff J-2O, and all federated partners well in advance of the potential crisis or anticipated military operation the relationship is designed to support. If the crisis at hand was unanticipated, federated partnerships can and should be proposed, coordinated, and activated in an ad hoc manner, providing the required, rapid, flexible surge capability in a prompt and efficient manner. Partners providing federated support will be considered in direct support of the supported combatant command J-2. **Specific command relationships will be developed as part of crisis federation planning. Federated relationships may include assigning certain partners a reinforcing mission (e.g., taking over support requirements from a supporting partner when the organization cannot continue its federated mission).** Once established, all preplanned intelligence federation agreements must be formalized in OPLANs, CONPLANs, or functional plans and periodically practiced during theater joint exercises.

b. The Joint Staff J-2O will adjudicate conflicting partnership requirements and facilitate the establishment of crisis intelligence federations, and is responsible for providing overall supervision, guidance, and assistance to the crisis intelligence federation process. The Joint Staff J-2O will coordinate the re-prioritization of support when necessary, including the relief of supporting partners when resources are no longer available to continue assigned crisis federation support. Figure III-5 depicts the process for crisis intelligence augmentation and federation support.

7. Intelligence, Surveillance, and Reconnaissance Concept of Operations

To facilitate the optimum utilization of all available ISR assets, an ISR CONOPS should be developed in conjunction with operational planning. The ISR CONOPS should be based on the collection strategy and ISR execution planning, and should be developed jointly by the joint force J-2 and J-3. It should address how all available ISR assets and associated tasking, processing, exploitation, and dissemination (TPED) infrastructure, to include coalition and commercial assets, will be used to answer the joint force's intelligence requirements. The ISR CONOPS should also identify and discuss any ISR asset shortfalls relative to the joint force's validated PIRs, and may be used as a vehicle for justifying a request for the allocation of additional national ISR resources. It should also require a periodic evaluation of the capabilities and contributions of all available ISR assets relative to the joint force mission in order to maximize their efficient utilization, and to ensure the timely release of allocated ISR resources when no longer needed by the joint force.

a. The ISR CONOPS is the first step to building an ISR Annex and consists of two parts:

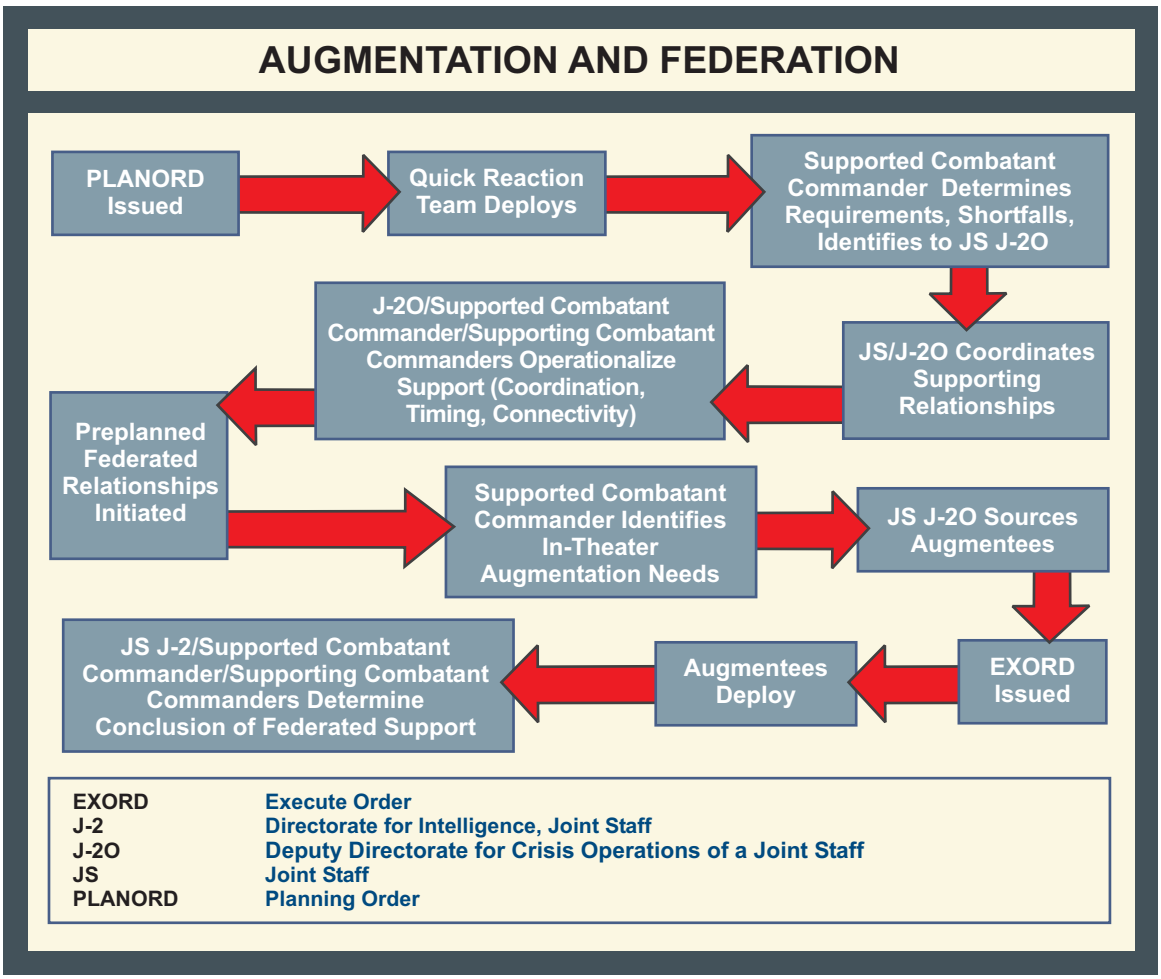


Figure III-5. Augmentation and Federation

(1) A brief description of validated intelligence requirements and ISR force organization, allocations, employment priorities, and command and control (C2) relationships.

(2) A general depiction of employed or planned employment of ISR assets to support daily joint and component-level operations.

b. The following are factors that should be considered when developing an ISR CONOPS:

(1) **Joint Force Commander (JFC Guidance).** The JFC translates strategic guidance into operational objectives necessary to plan and execute the military campaign. The JFC apportions the ISR effort based on campaign objectives. JIPB will assist in identifying gaps in the knowledge of the battlespace environment based on JFC guidance and mission analysis. Some of these gaps become the initial priorities for intelligence collection providing the baseline focus for planning ISR asset employment.

(2) **Commander's Critical Information Requirements.** ISR asset managers must understand the joint force's concept of operations. This includes routine monitoring of the commander's intelligence requirements and updated ISR guidance.

(3) **Collection Management Authority (CMA).** CMA may reside at the JTF level or may be delegated to components. In some cases, it may be a combination of both.

(4) **US and Coalition Theater and Tactical ISR** efforts should be integrated.

(5) **ISR Force Structure.** A key element is determining what the overall ISR assets requirements will be (i.e., is there a requirement for 24-hour SIGINT; how much IMINT and moving target coverage is needed?).

(6) **Distributed ISR Operations.** Distributed ISR operations, conducted from multiple independent nodes within an intelligence network, facilitate and enhance accomplishment of JFC objectives. The design of a distributed operation should enable a more survivable operation through distribution and sharing of assets and tasks while operating with common databases across a redundant communications network.

(7) **TPED Architecture.** Much of TPED necessarily occurs outside the theater via reachback and distributed architecture because vast intelligence requirements for first and second phase exploitation will quickly overwhelm in-theater assets.

8. Requirements-Based Intelligence, Surveillance, and Reconnaissance Resource Allocation

The mission may require ISR resources not organic to the theater or to the components of the subordinate joint force. ISR resources are typically in high demand and requirements usually exceed platform capabilities and inventory. **The joint force collection manager must ensure that all requests for additional ISR resources are based on validated needs as established by the command's formal intelligence requirements.**

a. The Commander, USSTRATCOM (CDRUSSTRATCOM) and Joint Staff J-2 and J-3 receive and analyze requests from combatant commands for additional ISR resources. Nonorganic ISR resources are allocated based on overall need as determined through the analysis and prioritization of validated theater intelligence requirements. In addition to optimizing ISR resource allocation, the requirements-based ISR resource allocation process also identifies critical unfilled requirements, and permits these requirements to be translated into programmatic recommendations.

(1) The USSTRATCOM ISR Division determines the optimum allocation of airborne ISR resources by evaluating the theater ISR CONOPS, consolidating theater intelligence requirements, analyzing the resulting collection need, modeling it against national agency databases, and ranking it against competing ISR requirements of other combatant commands. The USSTRATCOM ISR Division is assisted in the ISR resource allocation process through the use of the Airborne ISR Requirements-Based Allocation Tool (AIRBAT), a web-based automated tool that identifies the optimum allocation of airborne ISR resources by collating, analyzing, and comparing competing theater ISR requirements. The combatant commands help populate the AIRBAT database by furnishing USSTRATCOM and the Joint Staff J-2 with current, detailed, theater intelligence requirements, information requirements, and specific collection target data.

(2) The allocation process is informed by the global military force policy (GMFP) and/or Service identified metrics which identify allocable ISR resources for low-density, high-demand assets. The responsible Service provides limitations for assets not part of GMFP. Allocation recommendations that exceed metrics identified in the GMFP require approval by the Secretary of Defense.

b. CDRUSSTRATCOM recommends approval or disapproval of ISR allocation requests to the Joint Staff J-3. The Joint Staff J-3 staffs the recommendation via the Joint Staff deployment order (DEPORD) process and provides a final recommendation to the Chairman of the Joint Chiefs of Staff. Upon Secretary of Defense approval, the Chairman of the Joint Chiefs of Staff signs and promulgates the DEPORD.

SECTION B. COLLECTION

9. Overview

a. **Collection operations acquire information about the adversary and battlespace and provide that information to intelligence processing and exploitation elements.** Collection management, which occurs at all levels of intelligence, converts validated intelligence requirements into collection requirements; establishes, tasks or coordinates actions with appropriate collection sources or agencies; and monitors results and retasks as required. The foremost challenge of collection management is to maximize the effectiveness of limited collection resources within the time constraints imposed by operational requirements.

b. The terms "collection asset" and "collection resource" need to be clarified in order to understand the collection management process and the appropriate tasking procedures. **A collection asset or a collection resource is a collection system, platform, or capability. A collection asset is subordinate to the requesting unit or echelon, while a collection resource is not.** Requests for collection resources must be coordinated through the chain of command with the echelon that directs and controls them.

10. Principles of Collection Management

a. Collection managers develop collection plans based on validated intelligence requirements of commanders and decision makers. Intelligence analysts support the collection management process by identifying intelligence gaps and collection opportunities. **The collection manager's task is to first verify the requirements have been validated. Once verified, the manager begins the process to obtain the necessary information in response to the requirement.** To do this the collection manager:

(1) Develops and manages a collection plan that integrates requirements with target characteristics.

(2) Compares the plan to the capabilities and limitations of the available organic collection assets.

(3) Develops a collection strategy to optimize the effective and efficient use of all available, capable, and suitable collection assets and resources.

(4) In coordination with the J-3, forwards collection requirements to the component commander or national agency exercising tactical control over the ISR assets who will then task the asset to satisfy the requirement.

(5) Identifies collection requirements that cannot be met by organic assets and forwards them up the chain of command for validation and tasking of intelligence resources.

(6) Directs processing and dissemination of collected data. Collection managers must understand the capabilities and limitations of each discipline and the procedures for ensuring target coverage by the appropriate collection asset and/or resource. Collection managers keep requesters informed of collection status and capabilities so that there are realistic expectations of what can be collected and what level of confidence can be placed in the information.

b. Collection managers should follow four principles in all collection considerations (see Figure III-6).

(1) **Early Identification of Requirements.** Collection managers should be involved early in the identification and validation of requirements. Early consideration of collection factors enhances the ability to respond in a timely manner, ensures thorough planning, and increases flexibility in the choice of disciplines and systems.

(2) **Prioritization of Requirements.** Prioritization assigns a distinct ranking to each collection requirement. Collection decisions can be made rationally only if requirements are prioritized and the resulting trade-offs are fully understood. Time constraints and the finite number of collection, processing, and exploitation assets and/or resources mandate the prioritization of collection requirements. Prioritization, based on the commander's guidance and the current situation, ensures that limited assets and/or resources are directed against the most critical requirements. Collection requirements that are not time-sensitive may initially be submitted at lower priorities in the expectation that such requirements may be satisfied during complementary collection operations. If collection does not occur at the lower priority, the requirement should be reviewed for a possible increase in stated priority.

(3) **Multidiscipline Approach.** Collection disciplines complement each other, and the collection manager must resist favoring or becoming too reliant on a particular sensor, source, system, or technique. Each discipline's limitations can be mitigated through the capabilities of the others, as different systems provide additional insights into the requirement. While a sensor, source, and/or

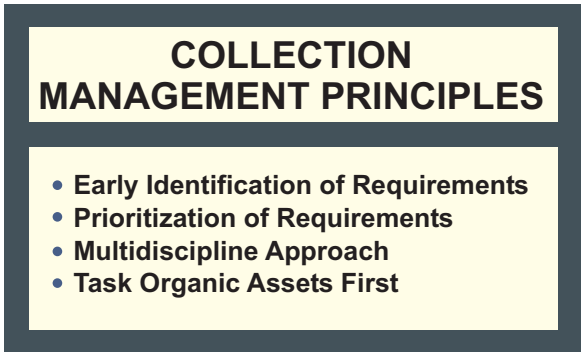


Figure III-6. Collection Management Principles

system may seem to be an obvious choice to satisfy a requirement, flexibility is the key. Collection managers are advised to match collection resources to the type of adversary activity most likely to be captured by collection operations to satisfy the information requirement. Rigid dependence on a single source may result in mission failure, especially if that source becomes unavailable or if the adversary becomes aware of the use of that single source and takes measures to counter it. Lack of a multidiscipline approach may also result in discernible patterns that may play into the adversary's CI or denial and deception (D&D) efforts.

(4) **Task Organic Assets First.** Use of organic collection assets allows a timely and tailored response to collection requirements and serves to lessen the burden on collection resources controlled by other units, agencies, and organizations. However, if requirements cannot be satisfied by organic assets, the collection manager should not hesitate to request collection support from higher, adjacent, and subordinate units, agencies, and organizations.

11. Collection Management

Collection management has two distinct functions: **collection requirements management (CRM) — defining what intelligence systems must collect; and collection operations management (COM) — specifying how to satisfy the requirement**. CRM focuses on the requirements of the customer, is all-source oriented, and advocates what information is necessary for collection. COM focuses on the selection of the specific intelligence discipline(s) and specific systems within a discipline to collect information addressing the customer's requirement. COM is conducted by organizations to determine which collection assets can best satisfy the customers' product requests (see Figure III-7).

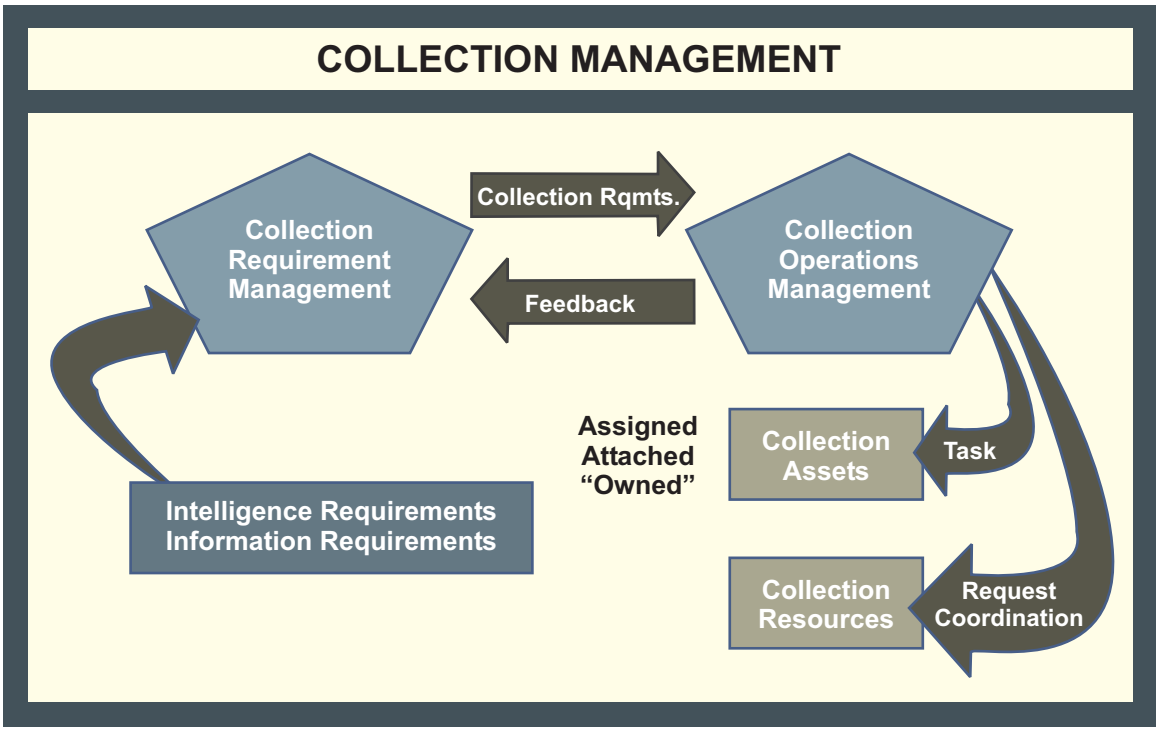


Figure III-7. Collection Management

a. Depending on the size of the collection management element, the CRM and COM functions may not be organizationally distinct. Although considered separately to facilitate understanding of their different objectives, in practice the distinction between them may disappear. There must be a constant dialogue between the two.

b. **COM and CRM are performed at all levels of the IC.** Each level interacts with the levels above and below, and among units, agencies, and organizations on the same level. The further up the chain, the broader the perspective and scope of responsibility; the lower, the more specific the function and narrow the scope. Organizations possessing collection assets and/or resources perform COM.

RELATIONSHIP BETWEEN COLLECTION MANAGEMENT AND OPERATIONS

The joint force commander's collection manager prioritizes collection requirements and recommends the appropriate asset to be assigned to collect against a particular target. The collection manager, in coordination with the operations directorate, forwards collection requirements to the component commander exercising tactical control over the theater reconnaissance and surveillance assets. A mission tasking order goes to the unit selected to be responsible for the accomplishment of the collection operations. The selected unit makes the final choice of specific platforms, equipment, and personnel based on such operational consideration as maintenance schedules, training, and experience.

SOURCE: Various Sources

12. Military Collection Requirements

Responsibility for military collection requirements management at the national level rests with DIA's Directorate for MASINT and Technical Collection (DT). The DT ensures that all-source collection capabilities are tasked to provide operational policy and intelligence support to the OSD, CJCS, the Services, combatant commands, subordinate joint forces, and their components.

a. To carry out these responsibilities, the DT coordinates and validates military collection requirements, including managing time-sensitive, ad hoc high interest and crisis-related all-source collection requirements for the Department of Defense. The DT develops all-source collection postures, strategies, policy and procedures, including providing advice on these subjects to the Director, DIA and Chairman of the Joint Chiefs of Staff as required for crisis response, intelligence issues, and other special events; evaluates the results of collection activities; and develops and maintains collection requirements databases and associated management systems.

b. The DT provides liaison and representation to facilitate cooperation with other intelligence and law enforcement agencies. The DT is the intelligence collection management interface with the Joint Staff Reconnaissance Operations Division for the review, coordination, and conduct of sensitive

reconnaissance operations worldwide. As consolidated authority for central HUMINT tasking, the DT coordinates and levies DOD HUMINT tasking and coordinates with other agencies responsible for SIGINT, IMINT, MASINT, and other special collection programs as required. Another function of the DT is to provide DOD and DIA representation on national-level forums charged with collection management and oversight responsibilities, such as the SIGINT Committee, as well as their subcommittees and working groups.

c. **In the event of war or periods of crisis, the President may direct the military to exercise greater responsibilities for tasking of collection systems.** When directed, national intelligence collection tasking authority may pass from the DCI to the Secretary of Defense. When this occurs, the DT manages this collection tasking authority. This collection tasking authority approves collection requirements, determines collection priorities, and resolves conflicts among collection priorities.

d. **Joint Staff J-2.** The other principal military member in collection at the national level is the Joint Staff J-2. The J-2 coordinates the tasking of national reconnaissance systems and nationally-subordinated manned reconnaissance platforms and sensors. The J-2 also responds to RFIs submitted by subordinate elements and commands.

e. **Operations Management.** Each of the intelligence collection disciplines has a separate infrastructure to manage operations.

f. **Theater Collection Management.** The theater J-2 must be kept apprised of all intelligence collection requirements being levied on assets and resources within the combatant command's AOR. **The theater J-2 retains full management authority (i.e., to validate, to modify, or to nonconcur) over all intelligence collection requirements within the AOR.** This authority may be delegated to a subordinate JFC. Collection requirements must be satisfied at the lowest possible level. Requirements that cannot be satisfied, and that have been validated by the command's collection manager or J-2, must be forwarded to the next higher echelon for action. This process continues until the requirement is satisfied, the intelligence is no longer needed, or it is determined that the requirement cannot be satisfied. Validated collection requirements and collection requests for theater and national systems will be forwarded for action to the theater intelligence collection management office. Validated collection requirements from components will become part of the theater collection plan and will be collected by theater collectors or forwarded to the DT.

13. Collection Requirements Management

Management and validation of collection requirement requests for a theater resides at the combatant command level. The validation process parallels that for RFIs and is responsive to operational requirements. The JIC validates and submits collection requirements to DIA if requirements cannot be satisfied by organic or subordinate assets.

a. **Requirements.** The subordinate joint force J-2 validates collection requirements and submits requests for additional collection resources to the combatant command J-2. The combatant command

J-2 validates or modifies standing collection requirements submitted by subordinate joint force or component commands. The JIC tracks the status of research, validation, submission and satisfaction of all collection requests received. **At the JFC's discretion, a joint collection management board (JCMB) may be formed to serve as a joint forum for the management of collection requirements and the coordination of collection operations.** The JCMB is chaired by the J-2 and should include J-3 and component representatives. If formed, the JCMB receives collection target nominations from the components and the JFC's staff, validates and prioritizes these requirements into a joint integrated prioritized collection list (JIPCL), and recommends the apportionment of organic ISR assets to meet JIPCL requirements.

b. **Collection Planning**

(1) **Collection planning is a continuous process that coordinates and integrates the efforts of all collection units and agencies.** CRM begins with initial efforts to answer the commander's PIR. Based on the PIR, intelligence analysts prepare RFIs. In the context of collection management, RFIs are queries to see if the information already exists and, if not, they form the basis of a collection requirement and/or analysis. The collection manager checks any ongoing collection operation that might contribute to satisfying the requirement. When previously collected information will not suffice, collection requirements will be developed. When the RFI manager positively determines that the information is neither available nor extractable from archived information or from lateral or higher echelons, an intelligence gap is identified. It becomes the responsibility of collection management to obtain the information.

(2) The collection plan may be either a simple hardcopy or automated worksheet used solely by the intelligence staff or a more formal document, depending on the complexity of the requirements to be satisfied. The collection plan includes statements of information desired, organic collection assets to be tasked or additional collection resources to be requested, when the information is needed, who is to receive the finished intelligence, and how it is to be used. The completed collection plan forms the basis for further collection actions (see Figure III-8).

(3) After establishing a collection plan, the collection manager transforms each requirement from the plan into a specific effort that ensures optimum employment of collection capabilities. For efficient management of collection requests, it is important to create, continuously update, and monitor a registry of active, prioritized requirements, such as the JIPCL.

c. **Resource Availability and Capability.** After defining the requirement, the collection manager determines the availability and capability of collection assets and resources that might contribute to requirement satisfaction. **The information sought is examined for discrete elements, called specific information requirements (SIRs).** A requirement may have more than one SIR. For each SIR, a set of key elements is developed that can be used to compare characteristics of the requirement's target with the characteristics of available assets or resources to determine collection suitability. Capability factors are shown at Figure III-9.

(1) **Key Element Sets.** Key elements are the parameters of the target's characteristics that can be compared with the characteristics of the available assets and/or resources and serve as

COLLECTION PLAN FORMAT

COLLECTION PLAN FORMAT

Period Covered: From_____ To_____

Priority or Other Intelligence Requirements	Indications	Specific Information Sought	Assets to be Tasked/ Resources to be Required	Place and Time to Report	Remarks

Figure III-8. Collection Plan Format

discriminators in discipline and/or sensor selection. A complete set of key elements provides the basis for identifying sensors fully capable of performing the collection task. The key elements commonly considered are: target characteristics, range to the target, and timeliness.

(a) **Target characteristics are the discernible physical, operational, and technical features of an object or event.** These characteristics may be observable and/or collectible. Observables are the unique descriptive features associated with the visible description of the target, whether it is specific units, equipment, or facilities. Collectibles are the unique descriptive features associated with emanations from the target. Observables are associated with IMINT and HUMINT/CI, collectibles with SIGINT, and both are associated with MASINT. One or more target characteristics may be associated with a specific information requirement, and these characteristics can be compared to a sensor(s) capability to collect. By continuing this process for each of the collection disciplines, a complete key element set is developed for the target.

(b) **Range** is measured as distance from a predetermined reference to the target location. The range to the target can be used to quickly eliminate from consideration both those standoff sensors that are unable to cover the target area and those sensors on penetration platforms not capable of reaching the target area. In HUMINT/CI, the analogous consideration would be source access.

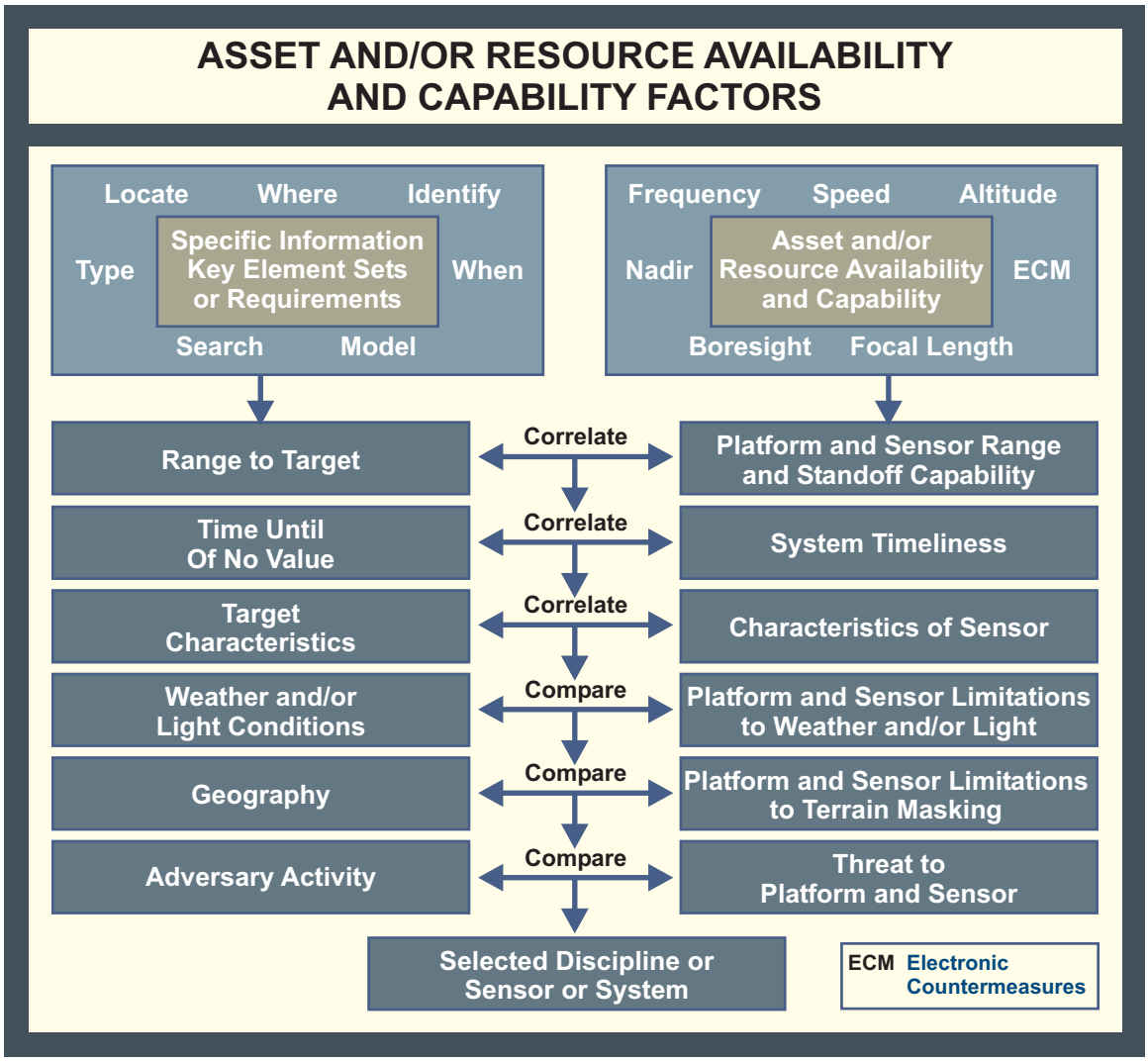


Figure III-9. Asset and/or Resource Availability and Capability Factors

(c) **Timeliness** is when the information requested must be received in order to be of value. In order to ensure timeliness, CRM planners must consider not only collection time, but also the lead time required for processing and exploiting collected data, and disseminating the resulting information.

(2) **Collection Capabilities Factors.** CRM translates the capabilities and limitations of the available sensors, systems, or disciplines into a set of collection capability factors that can be directly compared to the key element sets. The capabilities and limitations of various disciplines and systems are considered, together with their availability, to decide whether or not they should be tasked. **Sensor capability factors are technical or performance characteristics, range, dwell time, and timeliness.**

(a) **Performance characteristics** are concerned with the system's ability to collect the requested information, output quality, and location accuracy.

1. A system within a particular discipline may or may not be able to collect information on a particular target. For example, SIGINT collection systems operate in discrete frequency ranges, so that if the adversary system being sought operates outside those ranges, that particular collector is not viable as a potential source.

2. The data quality relates to the level of detail that can be derived from the collected information. For example, different imagery systems provide varying degrees of image resolution.

3. The importance of location accuracy depends on the planned use of the information collected. For example, information collected for targeting purposes demands greater locational accuracy than information collected for updating OB.

(b) **Range** deals with the system's ability to provide target coverage. For airborne systems, range is determined by considering the actual range capabilities of the sensor to provide detailed information sufficient to satisfy the requirement and the restrictions placed on the airborne platform, such as the maximum range capability of a platform to its downlink site. The CRM assesses combinations of these various range factors in order to determine a sensor's potential to meet operational requirements.

(c) **Dwell time** is the length of time a given collector can maintain access to the target, an important consideration in persistent surveillance, tracking, threat warning, and time-sensitive targeting scenarios, especially those involving mobile targets.

(d) **Timelines** consider the time required to complete each collection event, and is calculated or estimated for each available sensor based on the tactical situation and the local circumstances (see Figure III-10). Times vary depending on mission priority assigned, specific system availability, time required to plan the mission, and related information processing and dissemination means. These times are added to find an overall elapsed time, then compared with the latest timeliness requirements stated by the user. If the system's timeliness exceeds the latest time of receipt when the information collected will be usable, then it fails to contribute to satisfying the specific requirement and should not be considered for collection planning purposes.

(3) **Correlation.** Collection target characteristics are correlated with sensor capabilities. Specifically, key element sets are compared with collection capability factors to provide a preliminary list of sensors that are technically able to collect the desired data within the range to the target and time required.

(4) **Battlespace Factors.** After correlation, the candidate sensors are compared with battlespace factors to support final sensor selection. **Those battlespace factors include the threat, terrain, contamination, and weather that might influence the particular discipline or sensor selection.** Depending on the battlespace factors, a technically capable sensor may be dropped from consideration.

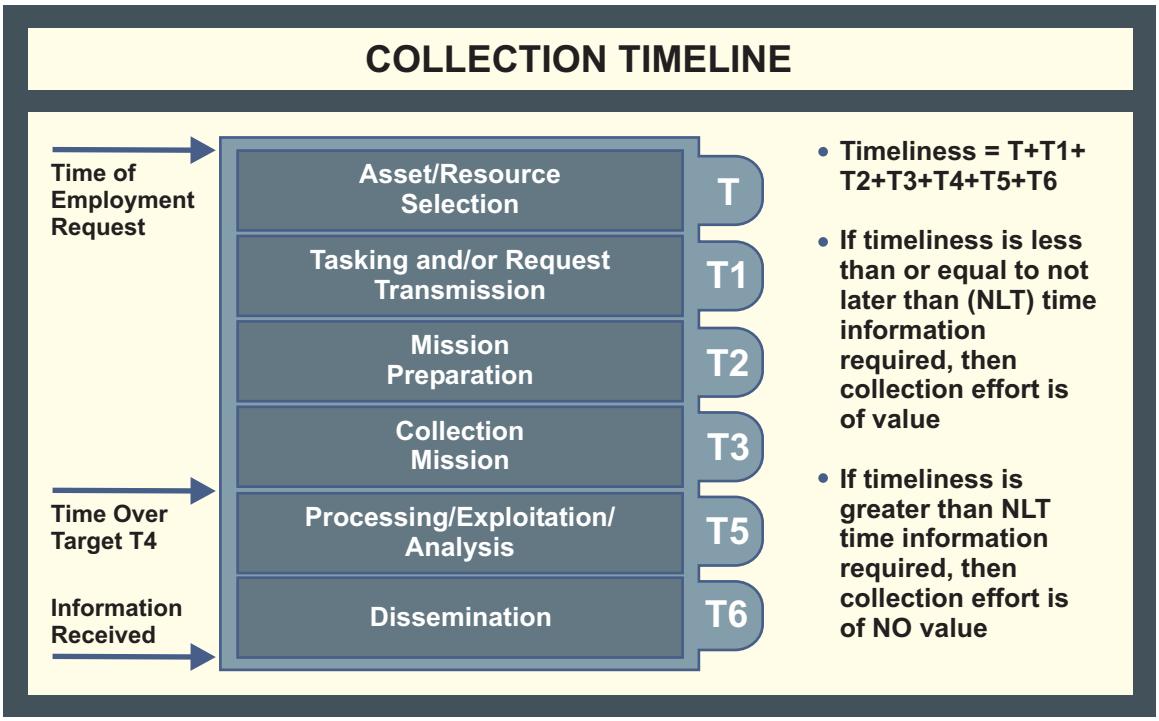


Figure III-10. Collection Timeline

(a) Sensor vulnerability is the degree to which adversary countermeasures may affect the collection platform and/or sensor. In general, the platforms of penetrating sensors are the most vulnerable, stand-off sensors less so, and satellite sensors the least vulnerable. Threat assessment is an evaluation of risk (military risk and political sensitivity) versus intelligence gain. When so designated by the commander, sensitive reconnaissance operations can be employed within predetermined, high-threat areas. Such operations require additional protective measures, some of which involve increased and/or specialized tasking of intelligence assets looking for adversary reactions that may require a threat warning alert.

(b) Weather and light conditions are also considerations, particularly with IMINT sensors. Weather conditions in and around the collection area affect the collection platform and/or sensor capability to collect data.

(c) Terrain is also a consideration. It may mask a target, thereby dictating both the choice of platform and the direction a sensor must point.

(d) WMD contamination may be present from the use of warfare agents, collateral damage, or release other than attack. Selection criteria for sensors must include their vulnerability to contamination, their ability to withstand decontamination, and their potential for spreading contamination.

(5) **Availability.** The list of viable collection disciplines, systems, and sensors is reviewed for current availability and the addition or deletion of capabilities. Coordination with adjacent and higher HQ will determine the availability of theater and national resources.

d. **Task Assets or Request Tasking of Resources**

(1) The collection manager begins by considering the highest priority requirement, then proceeds through the active requirements list to determine how each request can be satisfied (see Figure III-11). CRM transmits to COM the requirements and recommendations for planning, scheduling, and control of the prioritized list. The resulting tasking provides specific guidance that identifies the activity to undertake collection operations, the target to be covered, the date-time the mission is to be accomplished, and the place and time data is to be reported. **Collection tasking includes processing and exploitation tasking, guidance, and instructions.**

(2) **Collection to satisfy the requirement may occur at any level.** For example, if a combatant commander determines that the information needed to answer a RFI is unavailable, the commander may task organic collection assets or those of a subordinate organization or request multinational or national-level support to satisfy the requirement. When preparing the tasking and/or request, consideration should be given whether to integrate the requirement into an ongoing, planned, or new mission.

(3) Tasking request forms or messages are dependent on the tactical situation, type of sensor, and type of asset or resource (i.e., organic, supporting, theater, national, or multinational). Many specific data elements in these requests and the transmission procedures are classified. In the case of organic and direct support assets, requesters follow instructions provided in the OPLAN or operation order (OPORD) intelligence annex, or by message. In addition, the Joint Tactical Exploitation of National Systems Manual and the DIA 58-series manuals provide guidance for requesting support from national resources. In preparing requests for national resources, the collection manager should consider the guidelines in Figure III-12.

(4) **Intelligence Collection Strategy. A collection strategy is a systematic scheme to optimize the effective and efficient tasking of all capable, available, and appropriate collection assets and/or resources against requirements.** Collection system effectiveness is determined by analyzing the capability and availability of ISR assets and resources to collect against specific targets. Collection system efficiency is determined by comparing the appropriateness of all available and capable ISR assets to collect against specific targets in a given environment. For example, an RC-135 might provide a greater collection capability than is required to support a given mission. In such situations, an RU-21 Guardrail might be sufficiently capable of meeting the joint force's requirements, and would therefore serve as an appropriate substitute for the more capable RC-135, which could be more efficiently used elsewhere. The collection strategy considers all outstanding intelligence requirements, their relative priority, and the immediate tactical situation.

(a) **Resource integration** is a process whereby a new collection requirement is integrated with current or planned missions to increase the efficiency of the overall collection effort. By tasking a mission already in progress, it may be possible to reduce timelines, make collection more responsive to the request, and decrease cost and risk. This is weighed against the priority of scheduled targets that may have to be dropped to accommodate new targets and the impact of a mission change on the effectiveness of the ongoing mission. In cases where intelligence collection assets

COLLECTION TASKING WORKSHEET

COLLECTION TASKING WORKSHEET

Organization: **Registration Number:** _____

DTG: **Collection Manager:** _____

Specific Information Requirements: _____

Time: **Target Range:** _____

Characteristics: _____

Assets/ Resources	Range	Timeliness	Characteristics	Weather	Geography	Threat	Capability	Remarks
HUMINT								
CI								
IMINT								
COMINT								
ELINT								
MASINT								
TECHINT								

Assets/Resources Selected: HUMINT_____ COMINT_____ MASINT _____ CI _____

IMINT _____ ELINT_____ TECHINT_____

Figure III-11. Collection Tasking Worksheet

GUIDELINES FOR REQUESTING NATIONAL RESOURCE COLLECTION	
Areas of Interest	National systems are best employed against high-priority targets outside the range of organic or theater sensors, beyond standoff collection range, and/or in high threat areas.
Exploitation and/or Analysis Timeliness	Targets must be chosen such that, under applicable timeliness constraints, exploitation reports will reach the commander in time to react or influence decision making.
Justifications	Request justifications must fully explain the need for information and support the priority assigned by the requester.
Sensor Capabilities	Target descriptions must place minimum restrictions on systems' use.
Sensor Accessibility	The targets' accessibility must be determined when possible before a collection request is forwarded.
Exploitation and/or Analysis Requirements Clarity	Exploitation and/or analysis requirements must be concise, explicit statements of the actual information needed.
Exploitation and/or Analysis Requirement Purpose	Exploitation and/or analysis requirements must state the purpose of the information desired when it will benefit the interpreter and/or analyst.
Preplanned Collection	Preplanned target sets submitted in advance of an operation can relieve the workload and must be considered where the tactical situation permits.

Figure III-12. Guidelines for Requesting National Resource Collection

may augment and clarify ongoing threat warning events, a rapid intelligence gain/loss assessment must be made and agreed upon by J-2/J-3 planners for re-tasking of collection missions already in progress. Situations may warrant such dynamic re-tasking of intelligence assets to support the commander's urgent force protection as opposed to intelligence requirements. When integration of a new collection requirement with current or already planned missions is not feasible, a new mission should be planned.

(b) While one source may be suitable to collect against different requirements, in some cases multiple sources are necessary to satisfy a single, high priority requirement. **Cueing** is the use of one discipline or sensor to target collection by another sensor.

(c) **Asset mix and/or redundancy** uses a combination of assets of differing disciplines (asset mix) or similar disciplines (asset redundancy) against a high priority target. When the probability of success of one sensor to completely satisfy the requirement is lower than acceptable, the use of

multiple capabilities of different systems or disciplines increases the likelihood of success. Asset mix or redundancy places greater demands on the limited assets and/or resources available and has to be clearly justified by the potential intelligence gain.

(d) Across the range of military operations, collection strategies against high current interest targets should emphasize and provide for the near-continuous, all weather, day/night surveillance of the battlespace through the efficient utilization of all appropriate ISR assets in a persistent surveillance, as opposed to periodic reconnaissance, mode. **Persistent surveillance** enables the effective use of precision-guided munitions and is critical to countering the adversary's use of D&D. Long dwell ISR platforms such as the Global Hawk and Predator UAVs, distributed undersea and unattended ground sensors, battlefield surveillance radars, and special operations forces (SOF) have enabled a paradigm shift in which it is possible to provide near-continuous surveillance over large portions of the battlespace to monitor, track, characterize and report on moving objects and dynamic events. Persistent surveillance is facilitated by the effective integration and synchronization of all theater and national ISR assets and resources in a coherent collection strategy. Because persistent surveillance depends heavily on resources which are in high demand and usually few in number, requirements for persistent surveillance must be prioritized.

e. **Evaluate Reporting. The evaluation process tracks the status of collection requirements and provides feedback to the requesters.** Monitoring outstanding requirements ensures that orders and requests to collection activities are understood and the right information is being sought. When the collection results are provided, the collection manager evaluates the report(s) for completeness, ensures that the requesters receive a copy, and determines, in conjunction with the requester, if the requirement has been satisfied. Requester feedback establishes customer satisfaction, permits tasker deletion and frees collection assets and resources to be redirected to satisfy other active requirements.

f. **Collection Plan Update.** Based on the requester's assessment of requirement satisfaction, the collection manager reviews priorities for currency. The collection plan is updated to include retasking (if the requirement is not satisfied), adding new requirements, or canceling satisfied requirements.

14. Collection Operations Management

The COM process organizes, directs, and monitors the equipment and personnel that actually collect the data to satisfy requirements. COM develops strategies for collection against requirements in cooperation with CRM; predicts how well a system can satisfy requirements; evaluates the performance of the collection systems; allocates and tasks collection assets and/or resources and processing and/or exploitation systems; and monitors and reports the operational status of collection systems (see Figure III-13). **The COM process is directly linked to collection plan execution through ISR visualization.**

a. **Collection Mission Planning**

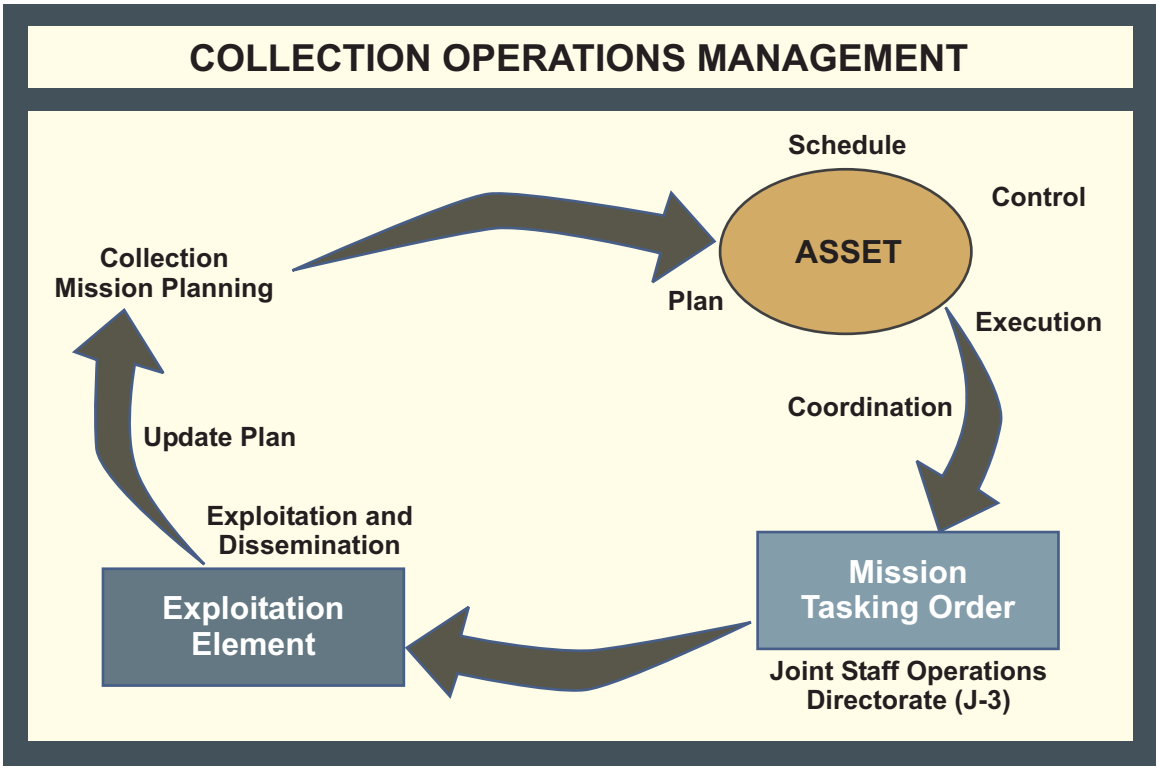


Figure III-13. Collection Operations Management

(1) Planning is concerned with the **identification, scheduling, and controlling of collection assets and/or resources**. The operations planner reviews mission requirements for sensor and target range, system responsiveness, timeliness, threat, weather, and reporting requirements. These elements are considered with the detailed technical, administrative, and logistic data of the collection system to identify and determine asset and/or resource availability and capability. The requirements are then translated into specific mission tasking orders.

(2) Effective coordination is vital in mission planning operations. With aircraft collection platforms in particular, many different staff elements are involved: operations, weather, maintenance and logistics, and communications must all be closely integrated into the mission planning effort. Intelligence sensor planners and managers of processing and exploitation elements must fully understand the requirements and mission profile. It is strongly recommended that COM personnel and resources be located in proximity to the operations staff elements which are responsible for reconnaissance assets.

b. **Execution.** A **mission tasking order** goes to the unit selected to be responsible for the accomplishment of the collection operation. The selected unit makes the final choice of specific platforms, equipment, and personnel based on such operational considerations as maintenance schedules, training, and experience.

c. **Exploitation.** Exploitation of collected information is closely associated with the management of collection assets and resources. **Generally the staff allocated a collection capability also**

controls the sensor-unique processing, exploitation, and analysis equipment. Exploitation is discussed further in Section C, "Processing and Exploitation," and dissemination in Section E, "Dissemination and Integration," of this chapter.

d. **Collection Planning Update.** Following exploitation, the report or processed data is disseminated to the requester. If the data is insufficient, the requester coordinates with the collection manager for additional coverage. At this point, the processed requirement transitions back to the CRM function. The collection manager and the exploitation manager, in coordination with requesters, continually assess how collection operations quality and timeliness may be improved. This effort relies heavily on those supporting organizations and other units or agencies that own and operate collection and exploitation assets or resources.

"Our satellites and platforms that collect ISR data had difficulty in a real-time, emerging target situation like we had in Kosovo. It's not that we can't do it, it's that we don't practice it . . . no target ever died in the collection process . . . we don't pop the cork when the picture arrives; we pop the cork when the target is dead."

General John Jumper
Commander, United States Air Force Europe, 1999

15. Intelligence, Surveillance, and Reconnaissance Visualization

ISR visualization is a subset of the COP available in the Global Command and Control System (GCCS) and Service command, control, communications, computers, and intelligence (C4I) systems. **It is an enabling capability within the COP that facilitates coordination and synchronization of ISR activities supporting the joint force and component commands.** This visual planning and decision-making aid is supported by a common data set of planning and execution information and by a process performed by the joint force and component command staffs that ensures continuous and responsive synchronization of current intelligence collection with current joint operations. The ISR visualization process is a J-2/J-3 and Service team effort intended to bridge the gaps between national, operational, and tactical level ISR systems and to fuse their activities to the joint force's operational tempo. ISR visualization facilitates a time-sensitive decision-making process driven by a rapidly changing battlespace. ISR visualization optimizes use of limited ISR collection assets, contributing near real time (NRT) ISR information that promotes persistent surveillance of the battlespace and enhances the JFC's battle management of the operation. Successful ISR visualization is contingent on timely reporting of ISR assets status, vigilant maintenance of the COP and its supporting data set, and successful integration with ISR asset ground station activities (see Figure III-14).

a. **ISR Display.** ISR visualization **provides an easily comprehended, readily accessible, graphic display that depicts the current and future locations of ISR assets, their capabilities, their field of regard, and their tasked targets**. ISR visualization requires continuous feedback regarding the current and projected locations of all ISR assets relative to their planned ground tracks. The ISR visualization display correlates in real time the collection status and location of all planned collection targets and the specific ISR asset tasked to collect on each target. ISR visualization displays

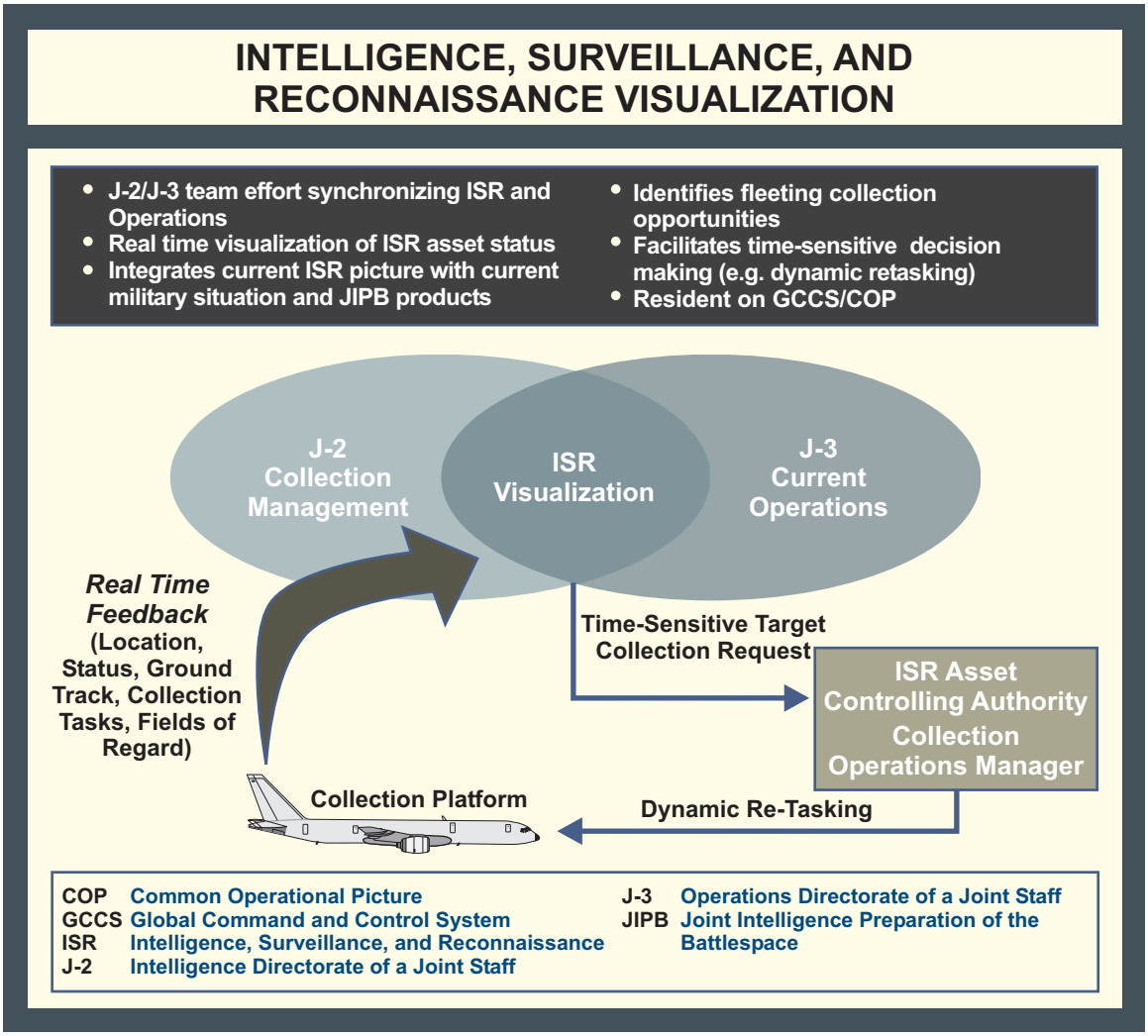


Figure III-14. Intelligence, Surveillance, and Reconnaissance Visualization

also depict the effects of the battlespace, to include METOC effects, on the collection capabilities of individual airborne ISR platforms as they progress along preplanned or ad hoc flight paths (e.g., the impact of terrain masking on sensor fields of regard at various altitudes). ISR visualization includes both collateral-level and sensitive compartmented information (SCI)-level displays.

b. **ISR Visualization and Current Operations. ISR visualization is integrated in NRT with current military operations.** From planning through execution, ISR visualization provides the J-2/J-3 a valuable tool for conducting ISR operations and rapidly responding to changing collection requirements. ISR visualization is merged with JIPB products such as event and decision support templates. The interface between ISR visualization and JIPB products is crucial and helps to optimize collection opportunities by projecting the possible future locations of adversary time-sensitive targets in time and space. Additionally, in order to assess the risk to ISR platforms, ISR visualization includes current intelligence overlays depicting changes in adversary counterair capabilities. ISR visualization facilitates the integration and synchronization of the joint force's and component commands' ISR activities and capabilities.

c. **Time-Sensitive Decision Making.** Based on the current military situation and the overall ISR picture, ISR visualization helps the commander and J-2/J-3 identify fleeting opportunities for intelligence collection or strike operations against adversary time-sensitive targets that may warrant dynamic re-tasking of collection platforms or re-targeting of strike assets. Additionally, time sensitive decision making is directly enhanced by ISR tasking and support to friendly force situational awareness and combat identification efforts. ISR visualization also helps to clarify ambiguous operational situations by optimizing the reconnaissance and surveillance of possible new targets or emergent, high-probability threats to friendly forces developed through intelligence tip-offs. At the request of, and in coordination with, the J-3 current operations staff, the J-2 collection management staff forwards a request for dynamic re-tasking to the controlling authority of the most appropriate ISR asset. The collection operations manager controlling the ISR platform accomplishes the actual re-tasking of the appropriate collection asset.

d. **ISR Visualization Architecture.** At the joint force-level, personnel performing ISR visualization maintenance in support of current operations should be fully integrated into the joint force J-3 current operations element, either through physical collocation or by virtual connectivity. Likewise, the joint force's ISR visualization operation must be integrated and interoperable with corresponding ISR battle management operations conducted at the component commands. **A common set of ISR visualization tools** provided through the joint GCCS and Service C4I variants must be fully integrated into these battle management operations and must support the commander's information requirements through the COP.

For a more detailed discussion of JIPB products and ISR, see JP 2-01.3, Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace.

SECTION C. PROCESSING AND EXPLOITATION

16. Overview

a. During processing and exploitation, **collected data is correlated and converted into a format suitable for subsequent analysis and production of intelligence**. Processing remains distinct from analysis and production in that the resulting information is not yet fully subject to analytical assessment. Nevertheless, **relevant time-sensitive information resulting from processing and exploitation (especially targeting, personnel recovery, or threat warning information) should be immediately disseminated through intelligence broadcasts, secure information workspace and/or internet relay chat channels, imagery product libraries (IPLs), intelligence databases, or message reporting**. These dissemination methods integrate processed data with existing information into the GCCS COP, providing a current view of the battlespace that facilitates time-critical decision making (see Figure III-15).

b. At the combatant command level, the J-2 manages theater processing systems and capabilities. Prior planning is critical to ensure preparation is made for system interoperability problems that may arise from a complex joint, interagency, and multinational systems and communications environment. The potential for operations involving both nonmilitary and nongovernmental organizations complicates this environment. The J-2 should consider these factors and be flexible in developing work-around

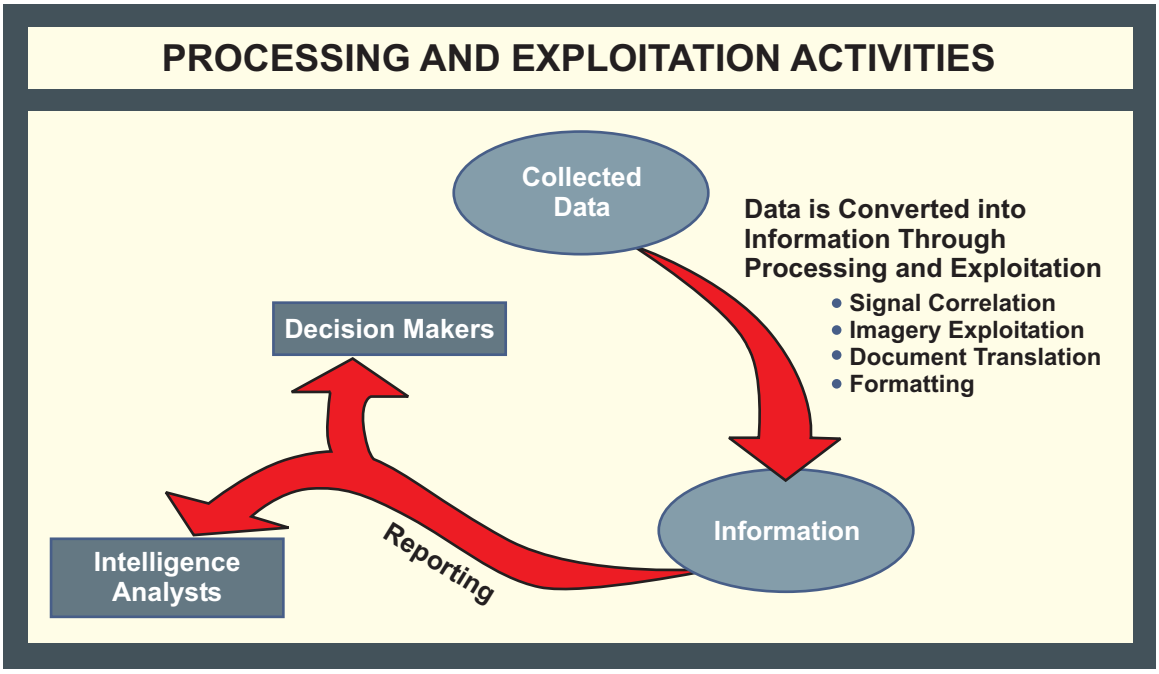


Figure III-15. Processing and Exploitation Activities

procedures. Intelligence processing elements should be prepared to set up both US-only and multinational segments.

c. Processing and exploitation of collected information by the components and their subordinate units is closely associated with the effective management of ISR assets. Normally, the collection operation element also controls the sensor-unique processing, exploitation, and analysis equipment. Various exploitation capabilities exist to service several different collection systems. The exploitation manager must plan the workload and develop a priority system for accomplishing the work, to include reporting status of ISR assets.

17. Human Intelligence

Processing of HUMINT information primarily involves **report preparation by collection activities at both the joint force and component levels**. Processing may also be accomplished within the joint force J-2X. Exploitation of human resource reporting is conducted by the JIC and joint force analytical and/or production activities; this primarily involves analyzing HUMINT reporting for inclusion in all-source production and/or for database maintenance. Components of the joint force may consider document exploitation and translation as HUMINT processing activities IAW Service doctrine, however, all captured documents should be forwarded to the J-2 DOCEX element for centralized processing and safeguarding.

THE CAPTURE OF THE GERMAN ROCKET SECRETS

Early in 1929, German engineers had begun studying rocket and jet propulsion to be used for transporting mail. In 1933, when Adolf Hitler became Chancellor, these studies were shifted to military uses, and the scientists were instructed to explore all ideas, however fanciful. Huge sums were made available to the Speer Ministry, where Dr. Wernher von Braun and a group of scientists conducted rocket research. The research enabled the "doomsday" weapons of the era to be produced, the best known of which were the V-1 and V-2 missiles.

In the Spring of 1945, as the outcome of WW II in Europe became more and more apparent, a principal focus of US intelligence units in Europe was to capture all possible information pertaining to rocket weapons. Accordingly these units followed closely behind advancing Allied forces, particularly in the Black Forest area where technical personnel with key documents from the Speer Ministry had scattered under heavy pressure of aerial bombing in Berlin. It was up to the intelligence units to find these individuals and gain information from them. The search began by interrogating the Germans who were in custody as a result of the Allied advance.

This method of collection, while painstaking, proved fruitful. Through such interrogations US intelligence officers learned that the former director general of German rocket production, George Richkey, was in captivity, working in a salt mine in the Black Forest. The following is the account of Norman Beasley, who told the story of his brother, Colonel Peter Beasley, the senior intelligence collection officer in the area.

"'I've got a job for you that is different than working in the salt mine,' Colonel Beasley told Richkey at the first interrogation. 'I want you to begin right now writing out a full description of yourself and all the activities of the V-2 factory.'

When Richkey's report was completed, Colonel Beasley made it clear, 'we accept you as an official of the German Government; we have patience and time and lots of people—you have lost the war and so as far as I am concerned you are a man who knows a lot about rockets. As an American officer, I want my country to have full possession of all your knowledge. To my superiors, I shall recommend that you be taken to the United States.'

Richkey nodded his assent, explained he was a scientist and wanted only to develop his knowledge in pleasant surroundings, such as the United States, and agreed to tell where the records were hidden, and to show the colonel the place.

Only hours later, under a heavily armed escort, Richkey led Colonel Beasley into the Black Forest to a cave, 5 feet wide and 5 feet high, running 300 feet into a mountain. There, records were found intact. Upon examination, the records disclosed basic blueprints, worksheets, engineering tables, and advanced plans for virtually every secret weapon in the possession of German scientists."

SOURCE: Norman Beasley, The Capture of the German Rocket Secrets Military Intelligence: Its Heroes and Legends, compiled by Diane L. Hamm US Army Intelligence and Security Command History Office, October 1987

18. Imagery Intelligence

Imagery may be processed and exploited at multiple locations simultaneously, both in and out of theater, by the JIC or equivalent, component command intelligence units, and national intelligence organizations. The JICs or equivalents, or other organizations, process the digital signal and display the downlinked imagery on a workstation in softcopy form for immediate exploitation. The imagery can also be stored on tape, sent to a digital library for later use, or laid down on film for exploitation on a light table. Imagery exploitation results, such as reporting and annotated images, may be incorporated into an all-source product focusing on a given target or target type, topic, or activity. IMINT may also be used to update databases resident with GCCS Integrated Imagery and Intelligence. Non-time-dominant exploitation results may be distributed via a hardcopy report, tape media (mailed or couriered to the user), or in electronic form.

19. Signals Intelligence

SIGINT support to joint operations includes communications intelligence (COMINT), ELINT, and foreign instrumentation signals intelligence (FISINT). **COMINT processing** is accomplished by NSA/CSS elements either assigned to or in support of the joint force mission. Depending on the level required for subsequent analysis and reporting, processing may be performed by assigned units in the operational area, at the regional JICs, or by specialized Service component or Defense activities. **ELINT processing** in support of a joint force may come from a number of sources including: assets attached to the joint force, national ELINT centers, and combatant command JICs. **FISINT processing** is accomplished by specialized, national-level Service and DOD organizations. Requests for SIGINT support should be forwarded through the theater J-2 to the NMJIC, and will result in tasking of appropriate organizations.

20. Measurement and Signature Intelligence

MASINT provides technically derived intelligence to detect, locate, track, identify, and describe the specific characteristics of fixed and dynamic target objects and sources. As an integral part of the all-source collection environment, MASINT contributes both a unique and complementary information component to the information requirements of commanders. Specialized MASINT processing and

exploitation techniques on collected raw data may be able to broaden the usefulness of data collected by other intelligence systems. **MASINT is employed as a global system with capabilities to exploit opportunities worldwide.** Service scientific and technical intelligence (S&TI) centers play a critical role in processing, exploiting and analyzing MASINT data. Additionally, the Services generate MASINT products in support of their respective components assigned to joint forces. The resulting MASINT products contribute to but are not limited to I&W, IPB, force protection, and foreign material exploitation. In addition, MASINT provides intelligence on WMD capabilities as well as weapons system capabilities based on analysis of collected telemetry data.

21. Open-Source Intelligence

Open-source intelligence (OSINT) is obtained from commercial radio and television broadcasts, newspapers, magazines, and other written publications. **OSINT processing transforms (converts, translates, and formats) text, graphics, sound, and motion video in response to user requirements.** For example, at the national level, the Foreign Broadcast Information System provides translations of foreign broadcast and print media. OSINT is also available from commercial companies which collect information using their own assets, or which buy information from independent contractors who listen to daily radio/television news broadcasts, and/or read daily newspapers.

22. Technical Intelligence

Exploitation of captured adversary equipment can provide critical information on adversary strengths and weaknesses that may favorably influence operation planning. **Exploitation of adversary equipment, excluding computer storage media, video and digital recording tapes, and media equipment, is generally performed in the combatant command by a joint captured materiel exploitation center (JCMEC)**, which is staffed by Foreign Materiel Program personnel from the Services' technical intelligence organizations and Naval Explosive Ordnance Disposal. Combatant commands or subordinate joint forces should notify the NMJIC through command channels when they require JCMEC support. This will ensure that appropriate Service component resources will be allocated.

Appendix G, "Joint Exploitation Centers," contains a more detailed description of the organization and responsibilities of a JCMEC.

23. Counterintelligence

Exploitation of data collected by CI assets can yield information critical to I&W and force protection. Additionally, law enforcement information or suspicious activity reports are important sources of information that need to be processed, exploited and fused with other CI sources. **Processing of CI information primarily involves report preparation by collection activities at both the joint force and component levels.** At the joint force level, this processing may also be accomplished within the J-2 CI/J-2X. When CI collection takes place in response to a requirement that has been generated from outside the CI community, the appropriate processed information will be reported in the form of an intelligence information report.

For more detailed information regarding CI processing, exploitation, and reporting, see JP 2-01.2, Joint Doctrine, Tactics, Techniques, and Procedures for Counterintelligence Support to Operations.

SECTION D. ANALYSIS AND PRODUCTION

24. Overview

a. Intelligence analysis and production is **accomplished in response to expressed and anticipated user requirements**. Intelligence (in the form of both products and services) responds to: the chain of command and the decision-making authority it supports; US policy decisions and military operational requirements; and changes in strategy, tactics, equipment, and overall capabilities of US and foreign military forces. Fused joint intelligence assessments, such as military capabilities assessments, military-related subjects assessments, or adversary COA assessments, are also frequently used to present the commander with the most thorough and accurate description and analysis of adversary capabilities, vulnerabilities, COGs, and probable intentions.

b. **Intelligence is produced through the integration, evaluation, analysis, and interpretation of information from single or multiple sources.** Intelligence production must be coordinated and directed by the J-2 to provide nonduplicative all-source intelligence products to the requester. Production for joint operations is accomplished by organizations at every echelon from national to subordinate joint force level. Effective production management ensures that the combatant commander and/or subordinate JFC receives the intelligence products and services required to accomplish the assigned mission. Automated database systems provide current tailorable data appropriate to the mission (see Figure III-16).

25. Conversion of Information into Intelligence

Information is converted into intelligence products through a **structured series of actions** which, although set out sequentially, may also take place concurrently. **These actions include the integration, evaluation, analysis, and interpretation of information** in response to known or anticipated intelligence production requirements.

a. **Integration.** Information from single or multiple sources is received, collated, and entered into appropriate databases by the analysis and production elements of IC organizations, the theater JICs or equivalents, or subordinate joint force JISE. Information is integrated and grouped with related pieces of information according to predetermined criteria to facilitate the evaluation of newly received information.

b. **Evaluation.** Each new item of information is evaluated by the appropriate analysis and production element with respect to the reliability of the source and the credibility of the information. An alphanumeric rating is assigned to each piece of information to indicate the degree of confidence the evaluator places on the information. This rating is based on the subjective judgment of the evaluator, the accuracy of previous information produced by the same source, and knowledge of the capabilities of particular

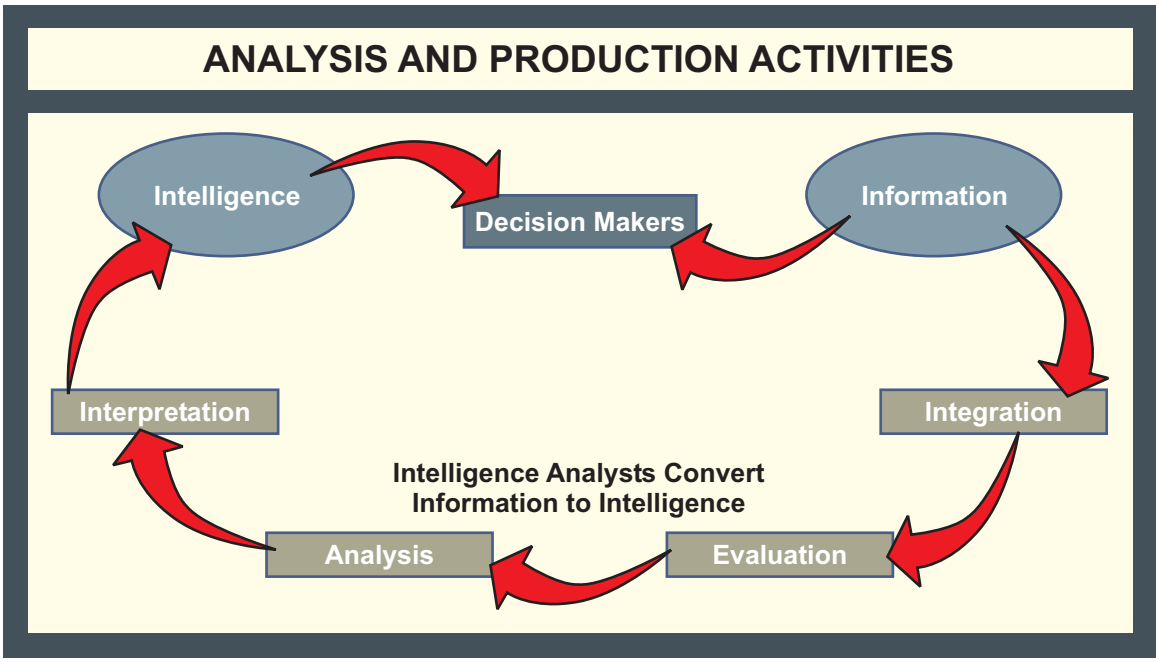


Figure III-16. Analysis and Production Activities

sensor systems. The reliability of the source and the credibility of the information must be assessed independently of each other to avoid the possibility of one factor evaluation biasing the other (see Figure III-17).

c. **Analysis.** During analysis, deductions are made by comparing integrated and evaluated information with known facts and predetermined assumptions. These deductions are combined and assessed to discern patterns or recognize events.

d. **Interpretation.** Interpretation is an objective mental process of comparison and deduction based on common sense, life experience, military knowledge covering both adversary and friendly forces and existing information and intelligence. This mental process involves the identification of new activity and a postulation regarding the significance of that activity.

26. Collaboration

a. Collaboration among intelligence producers is imperative not only to overcome shortages of analysis and production resources, but also to improve the overall quality of intelligence by providing access to recognized, but geographically separated, subject matter experts. **Through collaboration, intelligence analysts are able to share information, discuss opinions, debate hypotheses, and identify or resolve analytic disagreements.**

b. During crisis situations or contingency operations, some formal collaboration will be facilitated by preplanned federated intelligence partnerships. However, even in the absence of a federated support arrangement, JIC analysts and their counterparts in other theaters and at the national level should collaborate as the situational requirements dictate. During peacetime, routine, informal

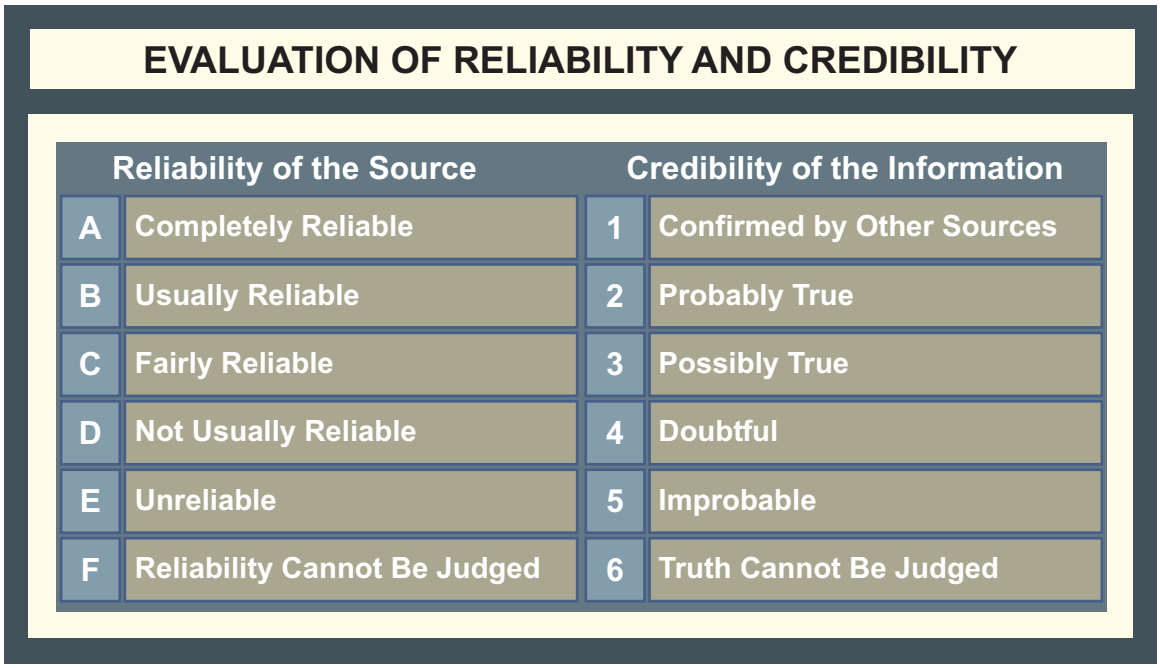


Figure III-17. Evaluation of Reliability and Credibility

collaboration among intelligence analysts should be encouraged within guidelines established by the JFC or joint force J-2.

c. The Joint Intelligence Virtual Architecture (JIVA) Collaborative Environment (JCE), which is accessible through JWICS and the SECRET Internet Protocol Router Network (SIPRNET), provides the primary means of collaboration among geographically dispersed intelligence analysts. JCE provides analysts with chat, instant messaging, data conferencing, web presentation, and knowledge management tools to create a virtual collaborative environment.

27. Databases and Virtual Knowledge Bases

a. **Intelligence databases are repositories of collected data, processed information, and finished intelligence products, and provide analysts with the technological means to rapidly retrieve, sort and correlate relevant information.** Intelligence databases are usually designed to support specific requirements and functions, and are therefore often "stovepiped" according to intelligence disciplines. For example the NGA National Exploitation System is the repository for imagery analysis and production, and the SIGINT On-Line Information System contains current and historical finished SIGINT products. The "stovepiping" of information by intelligence discipline or production category limits the potential timeliness and quality of intelligence production, as analysts are forced to search multiple databases for relevant information. Furthermore, as databases grow in volume and complexity, potentially vital pieces of information may become increasingly difficult for analysts to find and retrieve. In order to overcome this limitation, **virtual knowledge bases have been designed to serve as integrated repositories of multiple databases as well as reference documents and open-source material**.

Intelligence databases are described in greater detail in Chapter V, "Intelligence and the Global Information Grid."

b. **Virtual knowledge bases** are essentially databases of databases organized around geographical or topical "communities of interest." They provide the means for analysts and intelligence consumers to easily access the most current information and intelligence available in multiple databases and other reference sources. **Knowledge bases consist of elements (knowledge objects and knowledge packets) that can stand alone or be combined to make virtual documents that can be tailored to the users needs.** Knowledge bases logically organize intelligence issues in a hierarchy that facilitates analytic problem solving (see Figure III-18). Additionally, dynamic links among knowledge base elements make it possible to automatically and simultaneously update intelligence products as new information is received.

28. Products

Intelligence products produced by or for the subordinate joint force are described below and in Figure III-19.

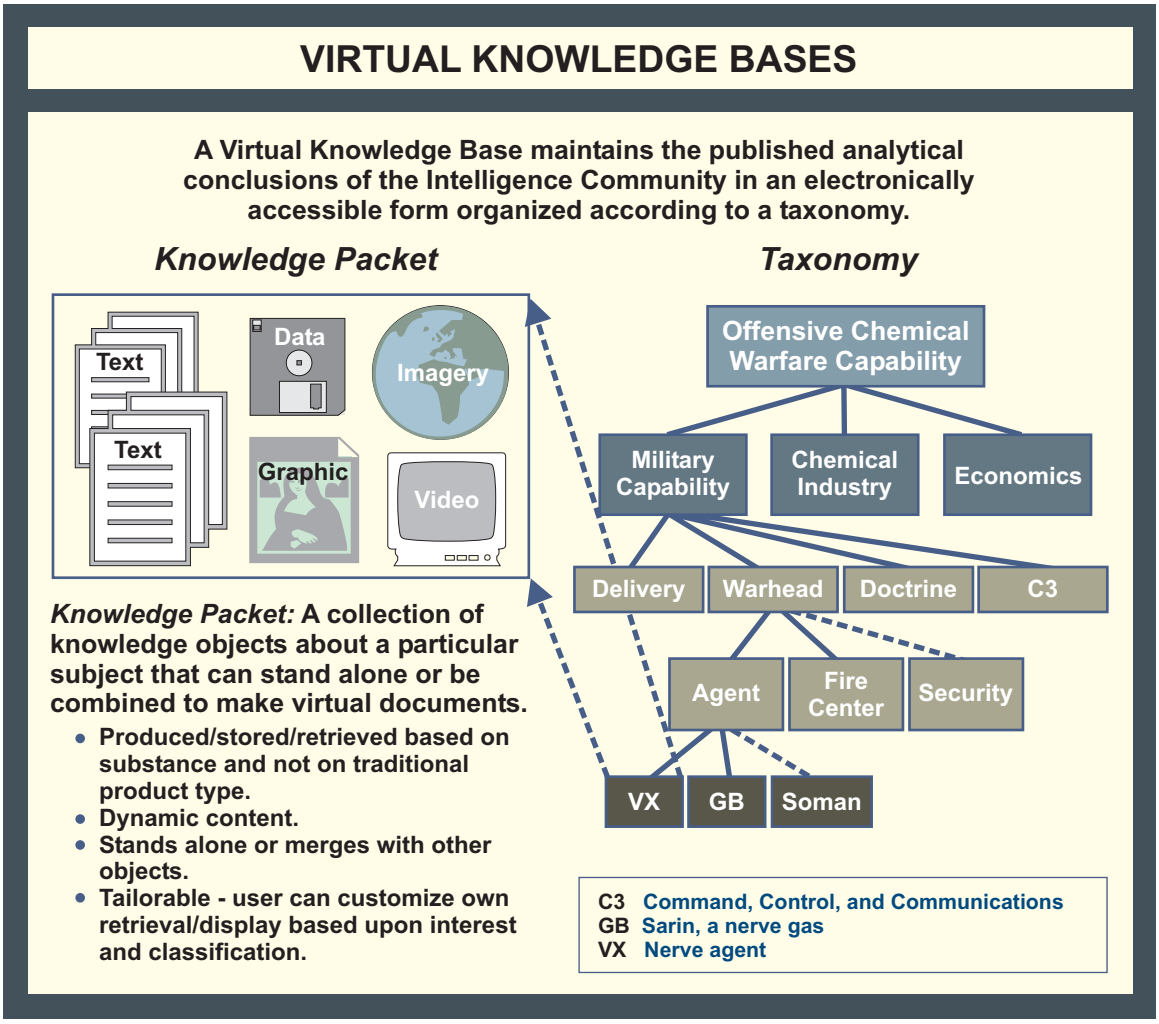


Figure III-18. Virtual Knowledge Bases

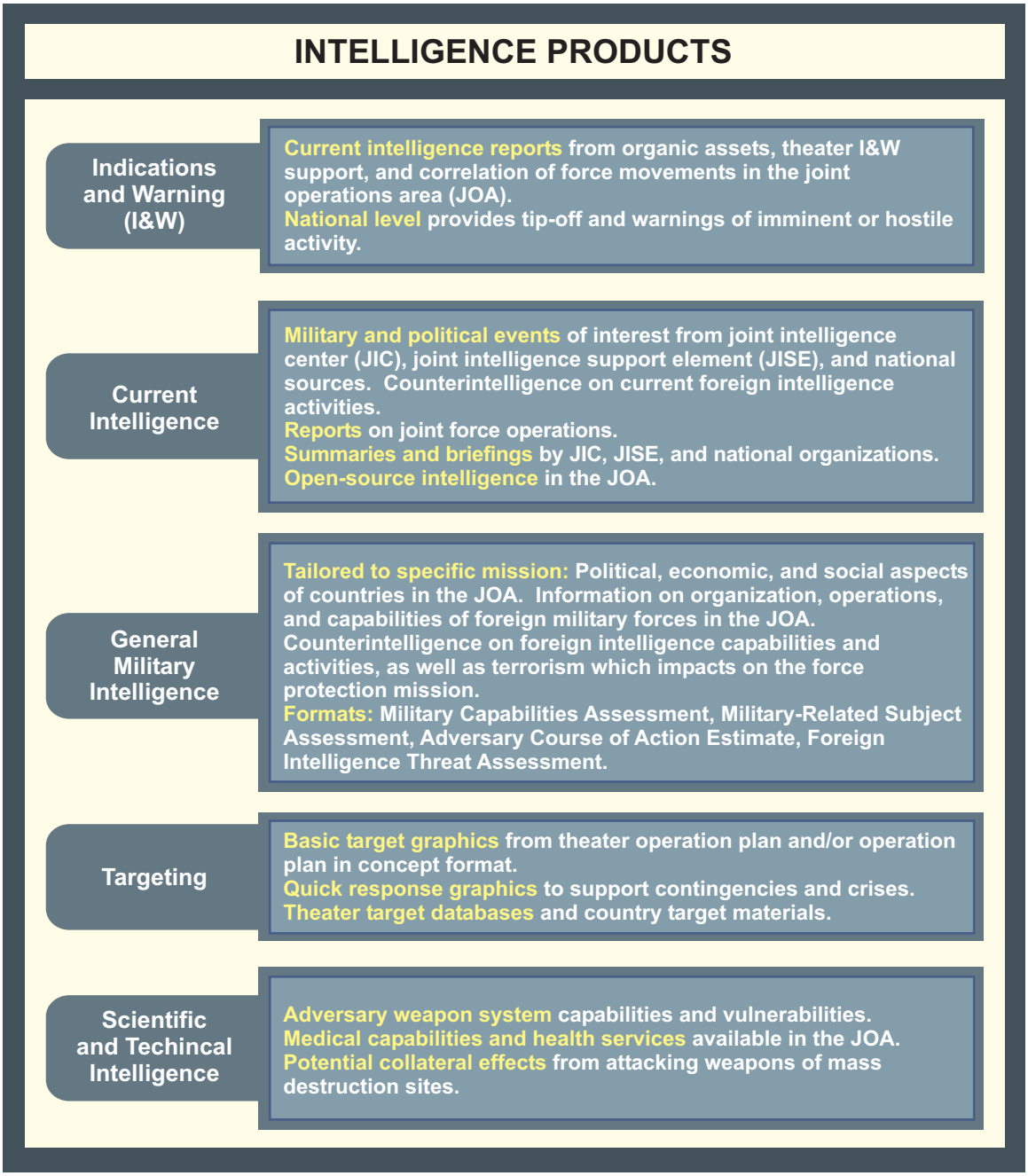


Figure III-19. Intelligence Products

a. **I&W**

(1) The I&W process analyzes and integrates operations and intelligence information to **assess the probability of hostile actions and provides sufficient warning to preempt, counter, or otherwise moderate their outcome**. The focus of I&W varies at each echelon, and is most specific at the operational and tactical levels.

(2) Subordinate joint force I&W relies on tip-offs from all sources at all levels. An integrated and responsive intelligence architecture must be established to satisfy theater requirements. I&W intelligence requirements include the following:

(a) Local or regional government capability to deal with the situation.

(b) Adversary intentions, capabilities, preparations, deployments and related activities, and possible methods of attack.

(c) Adversary motivations, possible triggering events, goals and objectives.

(d) Changes in adversary force dispositions, military activities, and mobilization status.

(e) IO capabilities in the region.

(f) Required military and civil mobilization preparations prior to military action taking place.

(g) Nonmilitary activity that could alter the situation, such as drastic changes in either friendly or opposing forces' political, economic or social situations. Other nonmilitary activities may include environmental factors such as weather, disease, and/or dispersion of toxic industrial materials (TIMs).

(h) Status of other military forces in the operational area.

THREAT WARNING

Threat warning is closely associated with, but functionally distinct from indications and warnings. Threat warning is the urgent communication and acknowledgement of time-critical information essential to the preservation of life and/or resources. The nature of threat warning is urgency. The sender of threat warning must always strive for acknowledgement of receipt of the alert. Although often times initiated by intelligence reporting and/or tip-offs, threat warning is an operations function that can be similarly initiated by operating forces, security elements, law enforcement, or civilian organizations. Different operational environments and situations lend themselves to different intelligence disciplines contributing to threat warning. Military operations in urban terrain may benefit from human intelligence-derived threat warning, whereas signals intelligence or measurement and signature intelligence-derived threat warning may prove critical during stabilization or air operations.

SOURCE: Various Sources

b. **Current Intelligence**

(1) Current intelligence involves **producing and disseminating all-source intelligence on the current situation in a particular area**. It is similar to I&W in that both depend upon continuous monitoring of world events and specific activities in the combatant command's AOR. The subordinate joint force receives current information from all levels of the IC.

(2) During the initial stages of an operation, the subordinate joint force J-2 should assess the adequacy of intelligence provided by the combatant command JIC and available through networked databases and submit prioritized RFIs to satisfy immediate intelligence needs and gaps in coverage. During sustained operations, the subordinate joint force's collection assets will be supplemented by theater and national support, to provide the joint force with current intelligence for use in intelligence assessments. Information required includes, but is not limited to the following:

(a) Adversary capabilities, probable intentions, and will to use military force, where, when, in what strength, and with what forces and weapons.

(b) The adversary's operational plans.

(c) The adversary's COGs.

(d) The adversary's vulnerabilities.

(e) Analysis of the operational area including terrain, hydrology, infectious disease and environmental factors, manmade features, demographics, and the location, type, and quantities of TIMs.

(f) Current and forecast METOC conditions which include the entire range of atmospheric phenomena extending from the earth's surface (cloud cover, precipitation, winds, and other METOC conditions) into space (space weather), as well as all of the marine environment from the bottom of the ocean to the air and/or sea interface (surf, sea conditions, or other sea interfaces).

(g) Military and political events.

(h) Status of strategic transportation nodes, to include major airfields, seaports, and surface networks.

(i) Adversary WMD assets, WMD-related facilities and activities (e.g., movement of WMD materials, technology and expertise to hostile states and terrorist organizations).

(j) Adversary foreign intelligence and security activities.

(3) Current intelligence and general military intelligence (GMI) efforts are interdependent. The intelligence gained during development of current intelligence forms the basis for the GMI effort.

c. **General Military Intelligence**

(1) GMI includes **pertinent information concerning the political, economic, and social aspects of foreign countries as well as all information on the organization, operations, facilities, and capabilities of selected foreign military forces**. GMI is tailored to specific subordinate joint force missions. Specifically, GMI deals with information on the items listed in Figure III-20.

(2) Fused joint intelligence assessments are listed below.

(a) **Military Capabilities Assessment.** Determining the adversary's potential military capability includes the identification of forces and dispositions, an evaluation of the adversary's vulnerabilities, and an assessment of the adversary's ability to employ military force to counter the objectives of friendly forces. The combatant command JIC is the subordinate joint force's primary source for all types of military capabilities assessments. Subordinate joint force components continuously provide information to the joint force JISE to update military capabilities databases. The five major components of an opposing force addressed in the assessment are as follows:

GENERAL MILITARY INTELLIGENCE CONCERNS

- **Adversary training, doctrine, leadership, experience, morale of forces, state of readiness, and will to fight**
- **Adversary's strengths and weaknesses, force composition, location, and disposition, including command, control, communications, computers, and intelligence, logistics and sustainment, force readiness and mobilization capabilities**
- **Basic infrastructure (power, resources, health, population centers, public infrastructure, and production and storage facilities for toxic industrial materials)**
- **Hydrographic and geographic intelligence, including urban areas, coasts and landing beaches, troop handling zones, and geological intelligence**
- **Capability and availability of all transportation modes in the operational area**
- **Military materiel production and support industries**
- **Military economics, including foreign military assistance**
- **Insurgency and terrorism**
- **Military-political and/or sociological intelligence**
- **Location, identification, and description of military-related installations**
- **Survival, escape, resistance, and evasion**
- **Government control**

Figure III-20. General Military Intelligence Concerns

1. **Leadership and C2.** An assessment of the adversary's ability to direct forces to accomplish a designated mission. Includes information on C2 nodes, lines of authority and reporting chains, and biographical data on key personnel.

2. **OB.** Identifies force components and assesses the strengths, structures, and dispositions of the personnel and equipment of the opposing military force, to include WMD.

3. **Force Readiness and Mission.** Assesses the adversary's readiness, as well as the doctrine it would follow and strategy and tactics it would employ, to achieve its objectives.

4. **Force Sustainability.** Assesses the ability of the force to logistically maintain the level and duration of combat activity (i.e., industrial, transportation and military infrastructure, supply status, attrition rates, and the adversary's morale) necessary to achieve objectives.

5. **Technical Intelligence.** Assesses the technical sophistication of forces, units, and weapon systems, to include WMD, as well as their capabilities, constraints, vulnerabilities, and countermeasures.

(b) **Military Related Subjects Assessment.** This type of assessment can provide indicators of an opposing force's capabilities and vulnerabilities, including its warfighting sustainability. Examples are as follows:

1. **C4 Systems.** An assessment of the adversary's C4 systems (i.e., telecommunications nodes and networks) to determine availability, connectivity, and vulnerabilities.

2. **Defense Industries.** An assessment of industrial production capacity, available stockpiles of goods and raw materials, natural resources, and reconstitution capability.

3. **Energy.** A listing of power sources and distribution network locations and capabilities.

4. **Military Geography.** A study of the impact that geographic features may have on planned operations, force deployment, and movement within the joint operations area (JOA).

5. **Demography.** Understanding the dispersion and cultural composition of the population (i.e., language, religion, socioeconomic status, and nationality or ethnic groups) in the operational area critical to the nature of the operations to be conducted.

6. **Transportation.** The lines of communications (LOCs) (i.e., location and capacities of airports, ports, and harbors; types, locations and capacities of roads, bridges, railways, and waterways) and equipment required by military, and/or civil-military related activities.

7. **Space Systems.** An assessment of the adversary's inherent and available space capabilities and infrastructure.

8. **Environmental Considerations.** Oil dumping, ignition of oil field fires; diseases and health threats (e.g., contaminated areas and availability of water supplies), and other environmental factors that could affect military operations. (The combatant command JIC is the primary source for the latest intelligence assessments of environmental considerations.)

9. **Medical.** Availability of foreign military and civilian medical facilities, equipment, and supplies as well as professional medical personnel to treat casualties. Infectious disease and environmental health risks, and scientific and technical developments in biotechnology and biomedical subjects of military importance. An assessment of preventive medicine efforts and the medical environment in which multinational forces will operate is important to ensure the correct medicine, clothing, and immunizations are available to the friendly forces and the local population. Particular attention must be paid to biological warfare (BW) threats because they may be difficult to detect. Due to the potential use of vectors, to include humans, and the limitations of automated BW detection systems, medical intelligence and epidemiological reporting may provide the first indication of a biological attack.

10. **METOC Support to Military Operations.** Climatology and METOC patterns affect friendly and adversary military operations. Understanding the opposing force's ability to assess METOC data is important in analyzing how the adversary may plan and conduct operations. For example, chemical and biological weapons effects are highly dependent on weather conditions. (The combatant command JIC or equivalent and the Joint METOC forecast unit or designated theater METOC unit are primary sources for assessing climatology and METOC patterns and the adversary's METOC capabilities.)

(c) **Multidisciplined CI.** Multidisciplined CI threat analysis evaluates all foreign intelligence and security services disciplines, terrorism, foreign-directed sabotage and related security threats. Analysis focuses on the JFC's ability to sustain forward operations and protect LOCs and main supply routes. Multidisciplined CI analysis includes detailed input to JIPB.

COUNTERINTELLIGENCE

Counterintelligence (CI) input to vulnerability assessments identifies weaknesses and vulnerabilities to friendly operations and activities that may be exploited by an adversary. CI input to threat assessments includes the current or projected capability of a foreign intelligence service to limit, neutralize, or negate the effectiveness of a friendly mission, organization, or material item through collection efforts, espionage, or sabotage. A personalities, organizations, installations and incidents database provides indications and insights into the motivations and ideologies of those who may come into contact with or influence the joint force's operational area. Investigative reports provide insight into potential weaknesses of foreign

intelligence services. A commander can request and use CI information to protect personnel, equipment, and facilities.

SOURCE: Various Sources

(d) **Intelligence Estimate.** Once a basic understanding of the threat and pertinent military-related subjects has been gained, it is necessary to try to view the situation through the adversary's eyes, visualize which COAs are available to the adversary, analyze the advantages and disadvantages of each from the adversary's perspective, and estimate which is the most likely option to be chosen. The intelligence estimate should also contain an assessment of all adversary COAs, especially the adversary's most likely COA and the COA determined to be most dangerous to friendly mission accomplishment. The joint force JISE and the combatant command JIC are the primary sources of information in support of these estimates.

Appendix D. "Sample Intelligence Estimate Format," provides a generic example of the format for an intelligence estimate."

d. **Target Intelligence.** Target intelligence portrays and locates the components of a target or target complex and indicates its vulnerability and relative importance. All-source analysis provides comprehensive targeting intelligence required for the commander to achieve operational objectives. **Target intelligence includes fixed and moving targets and provides analyses of construction (to support weaponeering) and signatures (to support target detection).** It is critical that intelligence analyses supporting targeting remain consistent throughout the joint force and component commands. The COP and its supporting Global Command and Control System Integrated Imagery and Intelligence (GCCS-I3) capability promote this unity of effort in providing a common set of data, information and intelligence. Targeting production requirements include the following:

(1) Adversary means, methods, goals, options, objectives, strengths, weaknesses, values, and critical nodes and elements as determined through target system and functional analyses.

(2) Target threat characteristics and vulnerabilities.

(3) Adversary COGs.

(4) Analysis of information warfare and other nonlethal weapons.

(5) Precise target location, construction information, and target signatures.

(6) Potential collateral effects such as release of TIMs or chemical, biological, or radiological material.

SPECIAL OPERATIONS TARGET INTELLIGENCE PACKAGES

The special operations target intelligence package (TIP) is developed by the theater joint intelligence center. TIPs contain timely, detailed, tailored, and focused multi-source information describing the target; the climate, geography, or hydrography; the demographic, cultural, political, and social features of the operations area; and the threat, to include strategy and force disposition of military, paramilitary, or other indigenous forces and security or police forces of danger to US elements. The TIP must also contain current imagery of the target and joint operations area, as well as accurate geospatial products and information.

SOURCE: Various Sources

e. **Scientific and Technical Intelligence. S&TI looks at foreign scientific and technical developments that have or indicate a warfare potential.** This includes medical capabilities and weapon system characteristics, capabilities, vulnerabilities, limitations, and effectiveness, research and development activities related to those systems, and related manufacturing information. S&TI collectors acquire adversary equipment and information in peacetime and war. The information is needed to preclude scientific and technological surprises and advantages by an adversary that could be detrimental to friendly personnel and operations. S&TI to support the research and development of friendly systems and countermeasures is gathered through foreign materiel exploitation, foreign materiel acquisition, and captured enemy equipment (CEE) programs.

29. Support to Operational Commanders

a. Combatant command, Service, and defense agency production centers will provide the Defense Intelligence Production Functional Manager with periodic status reports on their respective center's capability to meet assigned tasks. Production-related responsibilities of combatant command J-2s (see Figure III-21) include the following.

(1) To serve as overall shared production program (SPP) managers for their respective production center.

(2) To identify, consolidate, and validate command intelligence requirements for which intelligence production must be satisfied by maintenance and entry of data in SPP or command automated databases.

(3) To participate in production program reviews and other forums.

(4) To coordinate the tasking and assignment of production responsibilities to the production center within the command's chain of command. For areas outside the theater JIC capabilities and responsibilities, forward a request for production to the appropriate command, Service, or DIA.

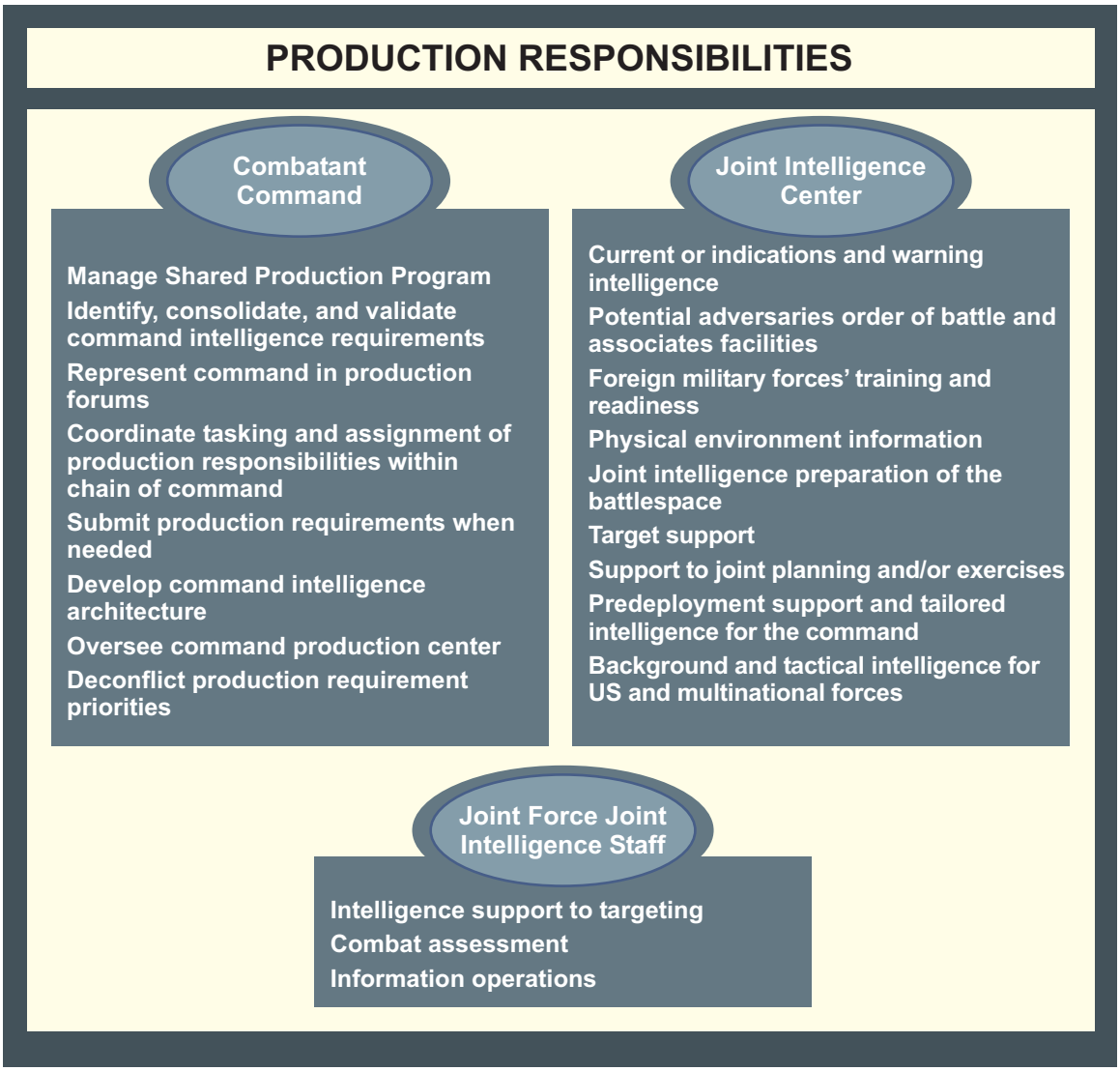


Figure III-21. Production Responsibilities

(5) To develop command architectures with the necessary capacity, connectivity, and processing power to host, manipulate, and exchange intelligence required to support command operations.

(6) To oversee activities of the command production center to ensure provision of timely, accurate intelligence to theater consumers and/or operators.

(7) To deconflict production requirement priorities.

b. **A combatant command's intelligence production is performed by a production center, or JIC, which is assigned directly to the combatant command in support of theater or specialized forces.** The JICs are the cornerstones for fulfilling the intelligence requirements of the geographic combatant commanders and their subordinate commanders. The JICs provide tailored, finished

intelligence products in support of theater mission planning and execution. Production-related responsibilities of the JIC include analysis and production of the following:

(1) Current and/or I&W intelligence for forces deployed in the command's AOR.

(2) Potential adversaries' OB and associated facilities and installations assigned under the SPP, to include assessing the general military capabilities of those forces.

(3) Foreign military forces' unit-level training and/or operational readiness.

(4) Physical environment information (including development of terrain analysis products) in areas of potential operations.

(5) JIPB in support of joint operation planning and ongoing operations.

(6) Target support, including development of target materials, BDA, weaponeering, target analysis, and special operations target intelligence packages.

(7) Information to support command-sponsored joint planning and exercises.

(8) Predeployment support and tailored intelligence produced elsewhere to meet the specific requirements of the command's customers.

(9) Background and tactical intelligence for customers within the theater, including US and multinational forces.

c. **Detailed intelligence is a critical requirement for conducting targeting. Responsibility for targeting resides with the JFC.** However, JFCs normally will delegate the authority to conduct execution planning, coordination, and deconfliction associated with targeting and will ensure that the process is also a joint effort involving applicable subordinate commands. The JFC's guidance directs and focuses operation planning and targeting to support the concept of operation. The joint force J-2 is responsible for intelligence support to targeting. The targeting process selects and prioritizes targets (geographical areas, installations, activities or facilities planned for capture, disruption or destruction by military forces) and matches the appropriate response to them, taking into account operational requirements and capabilities. Targeting entails the analysis of adversary situations relative to the mission objectives.

A detailed description of joint procedures for intelligence support to targeting is found in JP 2-01.1, Joint Tactics, Techniques, and Procedures for Intelligence Support to Targeting.

d. **Combat assessment (CA) is the determination of the overall effectiveness of force employment during military operations.** CA is composed of three major components: BDA; munitions effectiveness assessment; and reattack recommendation. Intelligence production support for CA includes detailed assessments of damage to the adversary's facilities and combat capability, summaries of adversary actions, predictions of adversary intent, analysis of collateral

damage, and recommendations for future operations. The J-3, with input from component commanders and the J-2, has primary responsibility for CA. During the planning and execution of joint operations, a critical responsibility of the J-2 is to accumulate, consolidate, and report battle damage inflicted on the adversary as a result of combat operations. Timely and accurate BDA facilitates current and future operations. BDA incorporates assessments of physical, functional, and target system damage. The JFC requires continuous feedback on the status of mission objectives, and operators need BDA input to determine the relative success of completed attacks, the necessity and timing of restrikes, and the selection of follow-on targets.

More information on CA can be found in JP 2-01.1, Joint Doctrine, Tactics, Techniques, and Procedures for Intelligence Support to Targeting.

HUMAN INTELLIGENCE AND TARGETING

"Identifying military targets was difficult [during DESERT STORM]; however, information acquired by human intelligence (HUMINT) operations improved targeting and destruction of significant military facilities in Baghdad, including the [Ministry of Defense] MOD and various communications nodes. In addition to blue prints and plans, HUMINT sources provided detailed memory sketches and were able to pinpoint on maps and photographs key locations, which subsequently were targeted.

Sources detailed the locations of bunkers underneath key facilities, including the Iraqi Air Force headquarters, which was composed of several main buildings and five underground bunkers, and the Iraqi practice of stringing coaxial communication cable under bridges rather than under the river beds in Baghdad and southern Iraq. This information was the deciding factor in the decision to target key bridges in Baghdad. Sources identified the communications center in Baghdad; less than 12 hours later, this facility was destroyed. Information obtained from EPWs [enemy prisoners of war] also helped planners direct effective air attacks against troops and logistics targets."

SOURCE: Final Report to Congress
***Conduct of the Persian Gulf War*, April 1992**

e. **IO targets information, information-based processes, and information systems.** The information system components consist of human factors, links and nodes. Offensive IO attacks an adversary's information infrastructure, erodes confidence in the information it provides, and enables commanders to operate within the adversary's decision-making cycle. Defensive IO protects the friendly information systems, maintains confidence in its ability to support operations, and shortens decision cycles. DIA and the national S&TI centers provide technical analytical support and parametric database information to the combatant commands in a variety of recurring and ad hoc documents and reports. Combatant commanders, component commanders, and subordinate JFCs plan and execute IO.

30. Production Responsibilities

a. Production centers at all levels are assigned clearly delineated areas of analytical responsibility across the range of military operations. These centers support the efficient use of production community resources, prevent duplication of effort, and provide timely support to customer requirements. **Production centers are designated as either primary or collaborative.**

(1) **Primary production centers produce the bulk of finished intelligence products.** A center designated as primary will be the authoritative source within the DODIPP for finished intelligence on designated topics and geographical areas.

(2) **Collaborative production centers** are designated because they possess a production capability distinct and unique from that possessed by the designated primary production center for the same topics and geographical areas. A center designated as collaborative will be the authoritative source within the DODIPP for finished intelligence on designated subsets of the topics and geographical areas for which the primary production center is responsible.

(3) Responsibilities of all production centers include:

(a) Accomplishing the required production for the specified combination of substantive topic (intelligence fusion center) and geographical areas.

(b) Identifying resources for the topic, including systems, funding, and specialists.

(c) Assuming lead or contributing production center responsibilities for validated production requirements.

(d) Requesting collection for any essential information gaps.

(e) Completing original research on the topic.

(f) Producing assigned categories in shared national-level databases (such as Modernized Integrated Database [MIDB]) within the topic and/or geographical area.

(g) Providing analysis and substantive judgments in response to validated customer requirements.

b. **The DODIPP** is structured to capitalize on the analytical and production resources of the entire DOD Intelligence Production Community (DODIPC) and to focus expertise and maximize output to the consumer. The structure is an explicit, logical division of activities, responsibilities, and accountability among national, Service, and combatant command production centers, and by the national-level military intelligence forums. SPP structure and procedures facilitate central management and decentralized execution of defense intelligence production. SPP is described more fully in Appendix F, "Department of Defense Shared Production Program."

c. **The combatant command J-2 identifies and validates command operational requirements.** The command's production center (JIC) schedules and accomplishes production activities for the theater, focusing on producing tailored, finished intelligence in support of theater mission planning and execution.

d. **At the subordinate joint force level, production focuses on the fusion of all-source intelligence from components, the combatant command JIC, and national sources to support the joint force mission and operations.** The combatant command JIC receives information from all echelons and performs all-source analysis and production. It is the primary source from which subordinate joint forces receive intelligence and intelligence products on their areas of interest.

e. **Lower echelons request, or pull, the tailored intelligence products they need from intelligence databases electronically available at intelligence centers at all levels.** This concept allows JFCs to acquire relevant intelligence, based on their mission and the specific phase of the ongoing operation, using intelligence databases physically maintained at other echelons and locations. The combatant command J-2 remains responsible for the coordination of intelligence information in-theater and manages the flow of intelligence through direct communication with each command and Service. The push and pull concepts are discussed further in Section E, "Dissemination and Integration."

31. Request Management

a. **Customers communicate requirements to their supporting intelligence office**, an existing military element or individual that serves DODIPC customers, which articulates the customers' needs as an RFI. RFIs state questions the customer wants answered or contain other specific intelligence needs, such as countries and topics required, in databases, target materials, and hardcopy or other production media. RFIs also specify the various levels of detail required as well as the periodicity of production and updates. An RFI template is contained in COLISEUM. COLISEUM automates the DODIPP procedures for registration and assignment of RFIs and subsequent tracking of the RFI.

b. After the supporting intelligence office surveys local resources to ensure the requirement does not duplicate existing or scheduled production, it completes and forwards the RFI to the validation office (VO) at the next level in the Service, combatant command, or DIA chain. **DIA/DI, each Service, and each combatant command has a VO to process and validate the PRs submitted by their organizations' supporting intelligence offices.** The validation process shall include a determination as to whether the requirement submitted by the supporting intelligence office has been properly identified as a PR or should be addressed by other means (e.g., as a collection requirement or request for personnel or operational support).

c. Upon validation, the VO determines if the requirement should be divided among multiple producers based upon the specifics of the PR and the expertise of the various production centers. The VO then assigns production responsibilities and transmits the assigned PR(s) to the appropriate production center(s) with information copies to possible collaborative production centers.

Simultaneously, information copies are sent to the Defense Intelligence Production Functional Manager (Director, DI).

d. Once requirements are assigned to a primary production center, the center coordinates the efforts of all collaborating production centers for the designated product. All centers schedule the production of each PR consistent with other assigned projects and DODIPP priorities. The commander and/or director of each production center is responsible for submitting a binding, for-the-record assessment of the center's ability to respond to each PR.

e. After coordination with collaborating centers, the primary production office provides a written interim response to the customer, stating the format and type of document it will produce and citing a final response date. Copies of the response are sent simultaneously to the assigning VO(s), the collaborating production centers, and the Defense Intelligence Production Functional Manager.

32. Prioritizing Requirements

a. **All requirements must be identified, documented, and prioritized.** Whenever possible, customer requirements should be satisfied with either existing intelligence products or modifications to existing products to prevent duplication of effort. Intelligence products must be in a format that the customer can understand and apply.

b. The subordinate joint force J-2 is the focus for all intelligence requirements generated within the joint force staffs and/or at lower echelons. These requirements are satisfied by the joint force J-2 through information the J-2 holds, can access via databases, or can acquire by organic collection assets. If internally generated requirements cannot be satisfied by organic joint force assets, the joint force J-2 shall validate and prioritize these requirements and submit them as RFIs to the combatant command JIC. This includes production and/or collection requirements that can be satisfied only by combatant command resources or by national agencies. If a combatant command JIC cannot satisfy these RFIs, it will forward them directly to the NMJIC for production or assignment to the appropriate national agency as necessary. Once RFIs and/or PRs have been submitted and accepted at any echelon, collection action is initiated as necessary. While the status of the RFI/PR is managed at each echelon, the subordinate joint force J-2 is responsible for tracking the status of joint force and component RFIs and ensuring feedback to components on the status of their requirements (see Figure III-22).

SECTION E. DISSEMINATION AND INTEGRATION

33. Overview

The timely dissemination of critical information and finished intelligence to appropriate consumers is paramount to attaining and maintaining information superiority. **Intelligence must be disseminated in such a manner that it is readily accessible by the user.** Time considerations dictate that information is "pushed" in a way that is automatically rendered or visualized in the GCCS COP. The integration of intelligence into the COP is facilitated by the GCCS-I3 mission

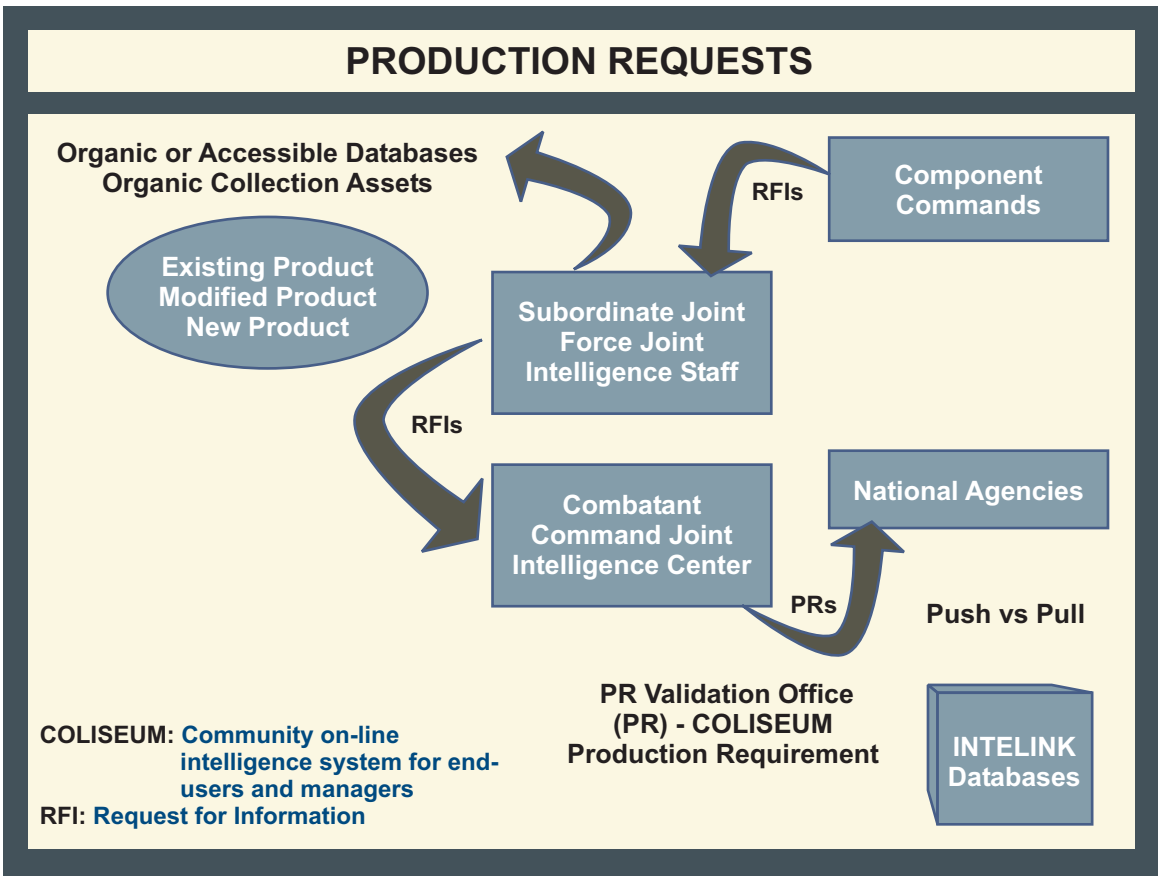


Figure III-22. Production Requests

application. GCCS-I3 enhances the COP by providing a standard set of integrated, linked tools and services which give ready access to imagery and intelligence that is seamlessly plotted on the COP.

a. **The J-2, at each echelon, manages the dissemination of intelligence to the user.** Intelligence must be provided in a form that is readily understood and directly usable by the recipient in a timely manner without overloading the user and, at the same time, minimizing the load on communications capabilities. It is also important to provide for maximum possible release of appropriate classified reporting, analysis, and targeting data to multinational forces.

b. **Dissemination consists of both "push" and "pull" control principles** (see Figure III-23). The "push" concept allows the higher echelons to push intelligence down to satisfy existing lower echelon requirements or to relay other relevant information to the lower level. This includes warning data initially received only at the national or theater level; other critical, previously unanticipated material affecting joint operations; intelligence which satisfies standing information requirements by a subordinate unit; or specially prepared studies requested in advance by the subordinate joint force J-2. **The "push" concept is managed through the Defense Intelligence Dissemination System (DIDS).** DIDS contains the intelligence consumer's statement of intelligence interest (SII). When a producer wants to push an intelligence product to the consumer, they query the DIDS database and create a distribution list. **The "pull" concept involves direct electronic access to databases, intelligence files, or other repositories by intelligence organizations at all levels.** An increasing number of intelligence

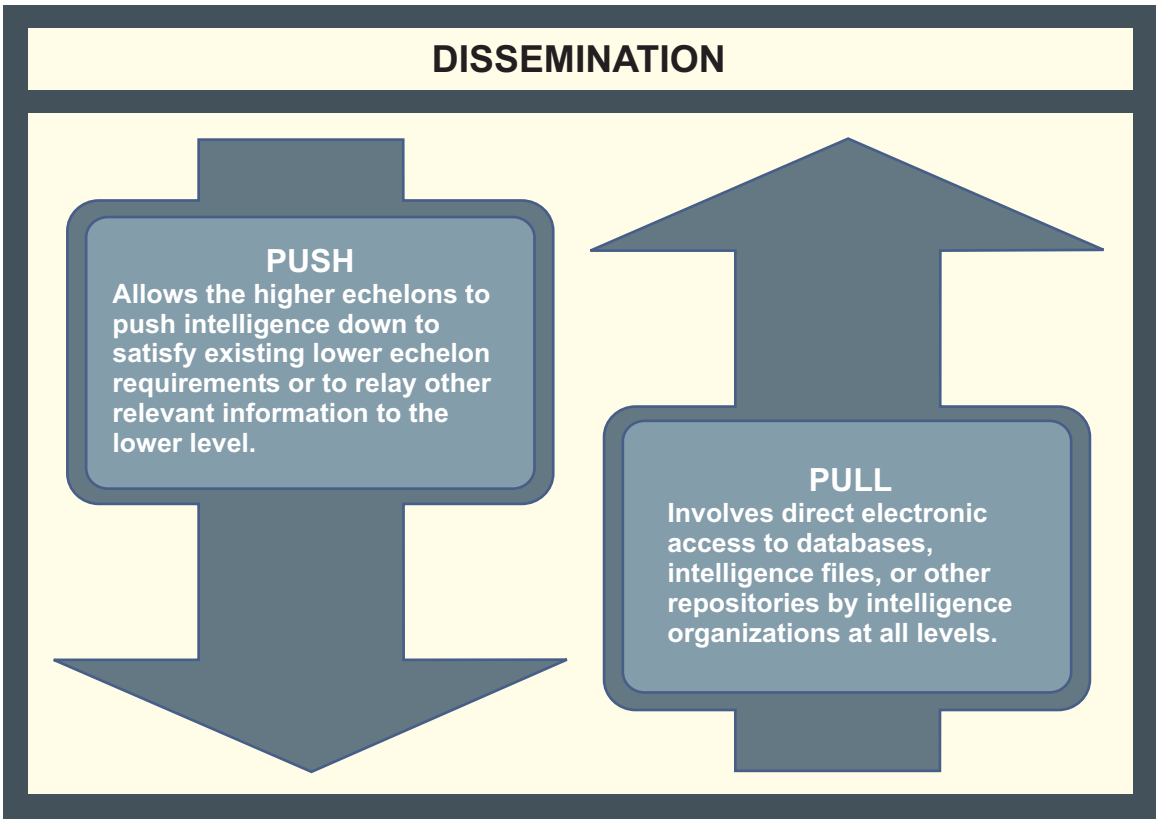


Figure III-23. Dissemination

"pull" products are available on INTELINK or INTELINK-S (collateral version), STONEGHOST (Commonwealth version of INTELINK), INTELINK-P (Policynet), and other national and theater file servers. The "pull" method is far quicker, and more preferred, than RFI/PR submission, provided the desired information already exists in a usable form. However, a judicious push may be needed to avoid overloading the lower, support HQ. The Global Broadcast Service (GBS) also provides a greatly enhanced capability to distribute multiple kinds of data, including bandwidth intensive video and imagery, to all levels of command. Additionally, the capability to directly broadcast threat warning alert notifications by means such as the NSA-provided TRIBUTARY voice threat warning network, enables the direct "push" of time-critical information from an ISR source to those friendly assets most at risk. Similarly, the utilization of information workspace and related capability of secure internet relay chat enables the collective "pull" of threat warning information by all subscribers.

c. During operation planning, the J-2 will coordinate with the J-3, logistics directorate of a joint staff (J-4), J-5, J-6 and component commanders to ensure that specific transportation assets, personnel, equipment (especially communications) and procedures (e.g., in-theater courier aircraft, vehicles, liaison teams, networked intelligence workstations, facsimile [FAX], voice, and other procedures) are available for disseminating intelligence and intelligence products within the AOR and/or JOA. The J-2's involvement during operation planning ensures his understanding of the intelligence products needed, required timeliness, consumer locations, and logistic and infrastructure assets available to support intelligence dissemination. This is particularly important when assets and infrastructure may be austere and LOCs extended.

d. **A key to operational success is the timely and accurate dissemination of intelligence to deployed units.** The dissemination manager ensures the efficient dissemination of intelligence products to the user. A dissemination program manager (DPM) works with the dissemination systems to get the product to the user. Dissemination managers, in cooperation with the combatant command's DPM, must ensure that appropriate mailing addresses, Defense Message System (DMS) message addresses and routing indicators, and special security office (SSO) security accreditation are requested and established for those units. This administrative information must be communicated to and validated by the command DPM, who will provide the information to DIA and other supporting national agencies. Further, the subordinate joint force J-2 should coordinate communications requirements with the joint force J-6 during the planning phase of the operation.

34. Dissemination Methods

a. **Softcopy Dissemination**

(1) **Softcopy dissemination has become the predominant method of communicating finished intelligence products to the consumer.** Publication producers and consumers have transitioned to an all-electronic product environment to improve the timeliness of intelligence dissemination and to reduce the amount of hardcopy distribution required. Reporting and archiving using electronic methods increase the IC's capability to use electronic means to deliver intelligence to operational forces. Communications tools such as the JWICS, SIPRNET, JDISS, Defense Intelligence Network, Open Source Information System (OSIS), GCCS, INTELINK and/or INTELINK-S, Integrated Broadcast Service via the GBS communications pipe are being integrated within the Global Information Grid (GIG) to deliver intelligence whenever and wherever required.

(2) JWICS and SIPRNET sites that have electronic publishing capability can pull electronic products. INTELINK and INTELINK-S constitute the IC architecture for sharing and disseminating intelligence, allowing organizations to have the ability to produce their own documents or contribute (collaborative publishing) to the creation of other documents throughout the electronic publishing community.

(3) Each J-2 site routinely has access to several daily current intelligence documents, including a variety of DOD and national agency products. Other documents (current and finished intelligence) as well as intelligence information reports and imagery are also being posted to servers (e.g., INTELINK, INTELINK-S, OSIS - unclassified only) for access by the combatant commands and subordinate joint forces. Other softcopy products include messages and intelligence databases maintained by national-level agencies or theater JICs.

(4) Electronic documents dissemination media varies (e.g., softcopy, compact disk-read only memory [CD-ROM], digital video disk), depending on the requirements of the end user. For example, JICs with INTELINK dissemination capability can pass the finished intelligence documents to their subordinate sites and/or create tailored intelligence products using CD-ROM or electronic publishing technology.

(5) Much of the material on INTELINK/INTELINK-S is available to anyone with access to a JWICS or SIPRNET terminal. With many documents already located on INTELINK/INTELINK-S, it may only be necessary for a site to tell the requester where the document exists. Requests for other existing electronic documents should be made directly via INTELINK or, if not directly accessible, the request should be directed to the appropriate DPM to satisfy the request. The softcopy document will in turn be placed either on the dissemination server for requester pull or electronic push.

(6) **The Services and combatant commands are integrating softcopy dissemination technologies into their intelligence architectures.** The subordinate joint force J-2 should quickly assess the equipment assets and training levels of all assigned forces to ensure timely dissemination of intelligence to all users.

(7) DOD and Service DCGS architectures are integrated components of the joint force intelligence processing and dissemination system. The DOD DCGS uses a "smart push/smart pull" concept which promotes bandwidth efficiency and is consistent with GIG precepts. It is designed to provide commanders with timely intelligence information derived from national, commercial, DOD, and combined force ISR nodes via a variety of point-to-point, broadcast, and web-based communications networks.

b. **Hardcopy Dissemination. The capability to deliver intelligence by FAX, message, or courier in hardcopy still remains a requirement in many situations.** In any operation involving allied or coalition forces, this is especially true as US intelligence equipment and system architectures are often not compatible or at the same security level. Additionally, some products, such as maps, are often available only in hardcopy when large quantities are required.

(1) Combatant commands manage the movement of hardcopy intelligence to deployed subordinate joint forces in coordination with the J-3, the J-4, the DPM, and the dissemination manager. Past operations and communication limitations associated with transmitting large format and/or color products have validated the continuing requirement to ship some critical hardcopy products, such as basic target graphics, to consumers.

(2) From the beginning of any operation, the combatant command, or subordinate joint force J-2, establishes a dedicated procedure for moving hardcopy intelligence from the production centers to the theater and distributing it within the AOR and/or JOA. This includes nominating priorities to the JFC relative to available air and/or sea lift resources for delivery of hardcopy intelligence support products.

35. Integration of Intelligence and Operations

Information superiority requires the timely integration of intelligence with operations in an easily understood format that facilitates decision making at all levels while at the same time maximizing the amount of relevant information available. Furthermore, the integration of intelligence and operations on a continuous basis allows commanders and all operational planners access to the most current information available, thereby optimizing intelligence support to operation planning, preparation, execution, and CA functions. **The primary vehicle for integrating intelligence and operations is the COP. Intelligence must be disseminated in such a manner that it can be automatically rendered or visualized in the COP and facilitate a shared operations/intelligence view of the battlespace.**

> *"Success in developing information superiority depends upon integrating information from a range of sensors, platforms, commands, and centers to produce all source intelligence. This intelligence must be part of a portrayal of the battlespace characterized by accurate assessments and visual depiction of friendly and enemy operations which makes the battlespace considerably more transparent for a United States commander than for the adversary and forms the basis for superior decision making. In short, intelligence must be displayable, digestible, and manageable. Interoperable will not be good enough. Integration into the Common Operational Picture is required."*
>
> **RADM L. E. Jacoby, USN**
> **Joint Staff J-2, 2001**

a. The GCCS COP is the integrated capability to receive, correlate, and display all available operationally relevant information, including planning applications and theater-generated overlays/projections. **The COP is a broad merging of inputs from a wide variety of tactical, operational and national sources into a single picture that serves a broad set of users for multiple purposes.** It facilitates decision making and planning at all levels, from Secretary of Defense policy decisions to joint force operation planning. **The COP depicts friendly, adversary, and third-party force dispositions and contacts on three types of graphical backgrounds**: vector maps (ordinary color graphic maps), digital terrain elevation data maps (topographical relief maps), and compressed ARC digitized raster graphics such as topographic and aeronautical charts. It includes a variety of NRT friendly and adversary air, ground and maritime tracks, threat/warning data, and intelligence broadcasts. Information received from the Integrated Broadcast System ELINT feeds from orbiting satellites and other passive ELINT sensors is automatically plotted on COP graphic displays. Additionally, operators can manually plot information received from other sources (see Figure III-24).

b. **GCCS-I3 provides the means for automatically integrating imagery and other relevant information and finished intelligence into the COP.** Areas of interest within exploited images may be annotated, cropped, and loaded on GCCS-I3 by national-level and/or combatant command intelligence organizations. After this initial download, GCCS-I3 is automatically updated with the latest imagery available in various IPLs. Metadata, such as basic encyclopedia numbers, should be added to these imagery files in order to facilitate linkage to OB databases, message traffic, and the air tasking order. This linkage between imagery and other collateral-level intelligence and operational databases

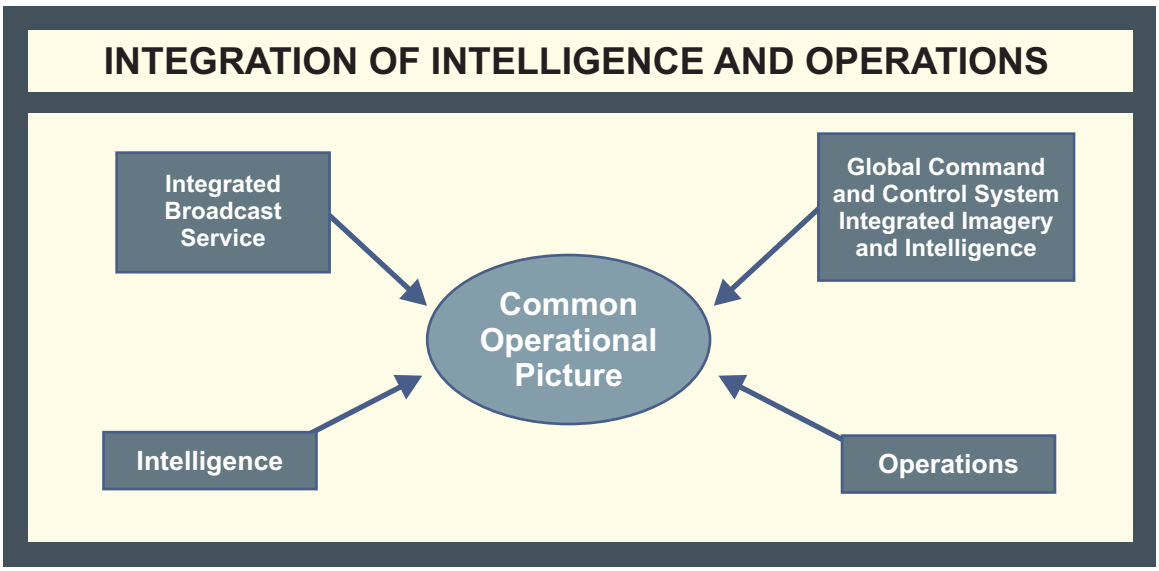


Figure III-24. Integration of Intelligence and Operations

facilitates intelligence analysis, battlespace awareness, operation planning, and BDA by providing intelligence **and** operations staffs with simultaneous access to the same information.

SECTION F. EVALUATION AND FEEDBACK

36. Overview

All intelligence operations are interrelated and the success or failure of one operation will impact the rest of the intelligence process. **It is imperative that intelligence personnel and consumers at all levels honestly evaluate and provide immediate feedback throughout the intelligence process on how well the various intelligence operations perform to meet the commander's intelligence requirements.** If the intelligence provided to the requester is complete, timely, and in a usable format, the requirement is satisfied and subsequently closed. If the resulting intelligence does not meet the above criteria, the requirement must not be considered satisfied and, time permitting, the requirement should be retasked for collection or production. Concurrently, remedial action must be immediately initiated to identify the reasons why the intelligence process failed to satisfy the requirement and to ensure such failure is not repeated.

37. Evaluation

All operations in the intelligence process are interrelated and must be evaluated to determine the degree to which they facilitate each other and ultimately succeed in meeting the customer's requirements. For example, planning and direction establishes the groundwork for all other intelligence operations, but it is also dependent on the results achieved by other operations in the intelligence process. The collection manager evaluates collection reports, ensures that the appropriate requesters receive a copy, and determines, in conjunction with the

requesters, if the requirements have been satisfied. Requester feedback establishes customer satisfaction and frees collection assets and resources to be redirected to satisfy other active requirements. Processing and exploitation, and analysis and production are evaluated based on the degree to which customers are satisfied that the resulting information or intelligence answers their requirements. Intelligence personnel and consumers at all levels evaluate the quality of intelligence products relative to all the attributes of good intelligence. These attributes include the degree to which intelligence anticipates the needs of the commander, and is timely, accurate, usable, complete, relevant, objective, and available (see Figure III-25). Finally, intelligence and operations personnel jointly evaluate how well intelligence is disseminated and integrated with operations, and make changes as needed to improve the overall intelligence process.

For more information on the attributes of good intelligence, see JP 2-0, Doctrine for Intelligence Support to Joint Operations.

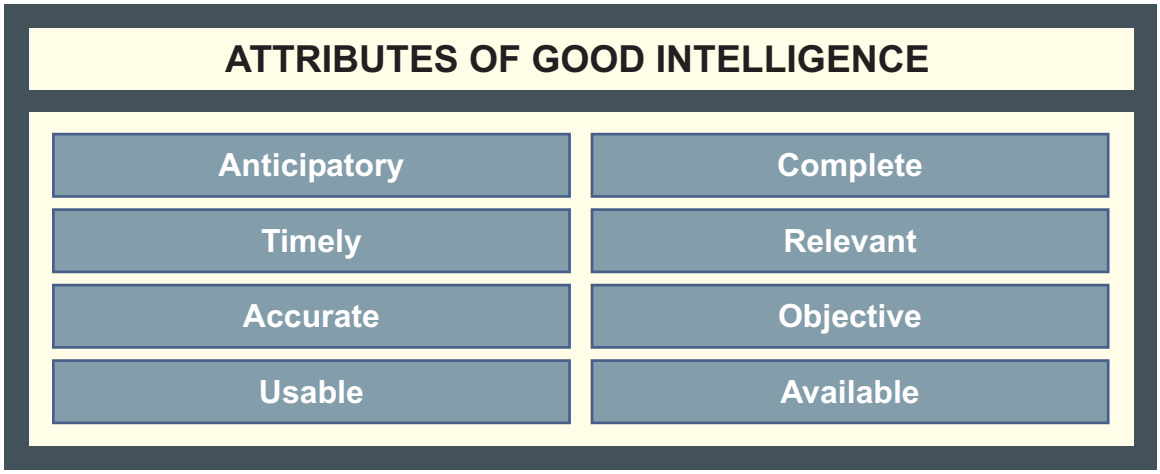


Figure III-25. Attributes of Good Intelligence

38. Feedback

All intelligence personnel and consumers are responsible for providing timely feedback to the joint force J-2 staff regarding both successes and problems with the functioning of the intelligence process. Inasmuch as all intelligence operations are interrelated, a functional problem in one type of operation can result in a ripple effect with ramifications for the intelligence process as a whole. It is therefore imperative that the J-2 staff initiate appropriate remedial measures as soon as feedback is received that identifies a current or potential problem. Additionally, the J-2 staff should periodically solicit intelligence personnel and consumers for ideas to improve the intelligence process.

Intentionally Blank

CHAPTER IV
INTELLIGENCE SUPPORT TO JOINT PLANNING

"One should know one's enemies, their alliances, their resources and nature of their country, in order to plan a campaign. One should know what to expect of one's friends, what resources one has, and foresee the future effects to determine what one has to fear or hope from political maneuvers."

Frederick the Great
***Instructions for His Generals*, 1747**

1. Introduction

a. In today's global threat environment, rigid sequentially-structured intelligence support to planning must yield to a more dynamic process involving overlapping and simultaneous activities. Military planners and decision makers require a faster, more accurate flow of information and intelligence. Intelligence support in this environment requires increased agility to quickly identify requirements, collect and disseminate information, and analyze and produce predictive intelligence to support the planning process. **Intelligence support to the joint planning effort must be focused to ensure that it fully anticipates and dynamically responds to the commander's requirements and the requirements of subordinate units and/or elements.** Sharing operational, communications and intelligence information among the J-2, J-3, J-4, J-5, and J-6 staffs is essential.

b. JP 5-0 series provides detailed information on planning joint operations. The Joint Operation Planning and Execution System (JOPES) provides the means to respond to emerging crisis situations or transition to war through rapid, coordinated, execution planning and implementation. JOPES translates policy decisions into OPLANs and OPORDs. JOPES formats can be found in Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3122.03, *Joint Operation Planning and Execution System Vol II: (Planning Formats and Guidance)*, and CJCSM 3122.04, *Joint Operation Planning and Execution System Vol II: (Supplemental Planning and Execution Formats and Guidance)*.

2. Intelligence Support to Joint Operation Planning

Intelligence support to joint operation planning includes a single integrated set of policies, activities, and procedures applicable to both deliberate planning and crisis action planning (CAP). Deliberate plans include OPLANs in complete format, CONPLANs with or without time-phased force and deployment data (TPFDD), and functional plans. CAP is conducted for the actual commitment of allocated forces, based on the current situation, when a contingency response is imminent. This planning results in time-sensitive development of campaign plans and/or OPORDs for execution. With the release of Contingency Planning Guidance (CPG) 04, combatant commanders are tasked to develop their OPLANs under an Adaptive Planning System prototype. Adaptive planning is the systematic, on-demand, creation and revision of executable plans, updated, as circumstances require. What sets adaptive planning apart from the current JOPES process is the significantly truncated development time and emphasis on collaborative

tools that allow parallel and concurrent planning to occur at the strategic and operational levels. As with any planning process, though, adaptive planning still entails time-tested decision-making fundamentals such as mission analysis, development of assumptions, and concept/course of action development. Likewise, the role of the intelligence staff planners does not fundamentally change in the adaptive planning process; the requirement for reliable intelligence and timely I&W will always be instrumental to any planning process. For purposes of illustration, the role of the intelligence staff in supporting operation planning is described in the notional process below.

a. **Strategic Guidance.** Combatant commanders plan against specific tasks in the CPG and Joint Strategic Capabilities Plan (JSCP), but also strive to anticipate additional situations in which the employment of US forces may be necessary. In general, strategic guidance provides long-term as well as intermediate or ancillary objectives. It should define what constitutes success (ends), describe the method of employing military force (ways), and allocate adequate resources (means) to achieve strategic objectives. As such, strategic guidance normally contains the following elements: strategic end state, resources, restraints, constraints, and strategic assumptions. These elements form the basis for subsequent planning to translate strategic guidance to military strategic objectives that define the role of military forces in the larger context of national strategic objectives. For additional guidance, see JP 5-0, *Doctrine for Planning Joint Operations*.

b. **Situation Development.** Situation development is a dynamic process that evolves simultaneously with policy (see Figure IV-1). **Intelligence supports situation development by identifying intelligence requirements, developing a collection plan, monitoring I&W problem sets, analyzing adversary activity, and providing intelligence assessments of adversary capabilities, vulnerabilities, COGs, intentions and possible COAs.** Effective situation development requires intelligence planning that is collaborative, adaptive to changing conditions, and anticipates the needs of the commander. The intelligence effort during situation development focuses on intelligence collection, I&W, and JIPB to illuminate the situation for the combatant commander, components, subordinate JFCs, OSD, and Chairman of the Joint Chiefs of Staff. The command J-5, with the assistance of the J-2, reviews existing plans to determine if the particular event driving the operation planning effort has been considered in deliberate planning. If an existing plan does not apply, the commander will need to develop PIRs tailored to the mission early in the planning process to assess intelligence information gaps. Preliminary recommendations on the appropriate JTF composition should be considered at this point. The combatant command J-2 should notify DIA, NSA, NGA, the Defense Information Systems Agency (DISA), the Joint Staff J-6, and any other relevant theater and national activities of requirements for intelligence, communications support, and manpower and equipment augmentation. The command J-2 should coordinate closely with the command J-3 and J-6 to ensure that these communications requirements receive sufficient priority in the command plan. Working with the command J-6, the command J-2 develops a subordinate joint force J-2 communications intelligence architecture that achieves interoperability laterally, vertically, and, if required, with multinational forces. It is also critical that intelligence planners work closely with their J-3, J-4, and J-6 counterparts to ensure priority for an early intelligence capability in support of deployed forces. Intelligence personnel, equipment, and communications paths must be part of the lead element in deployments to provide the commander

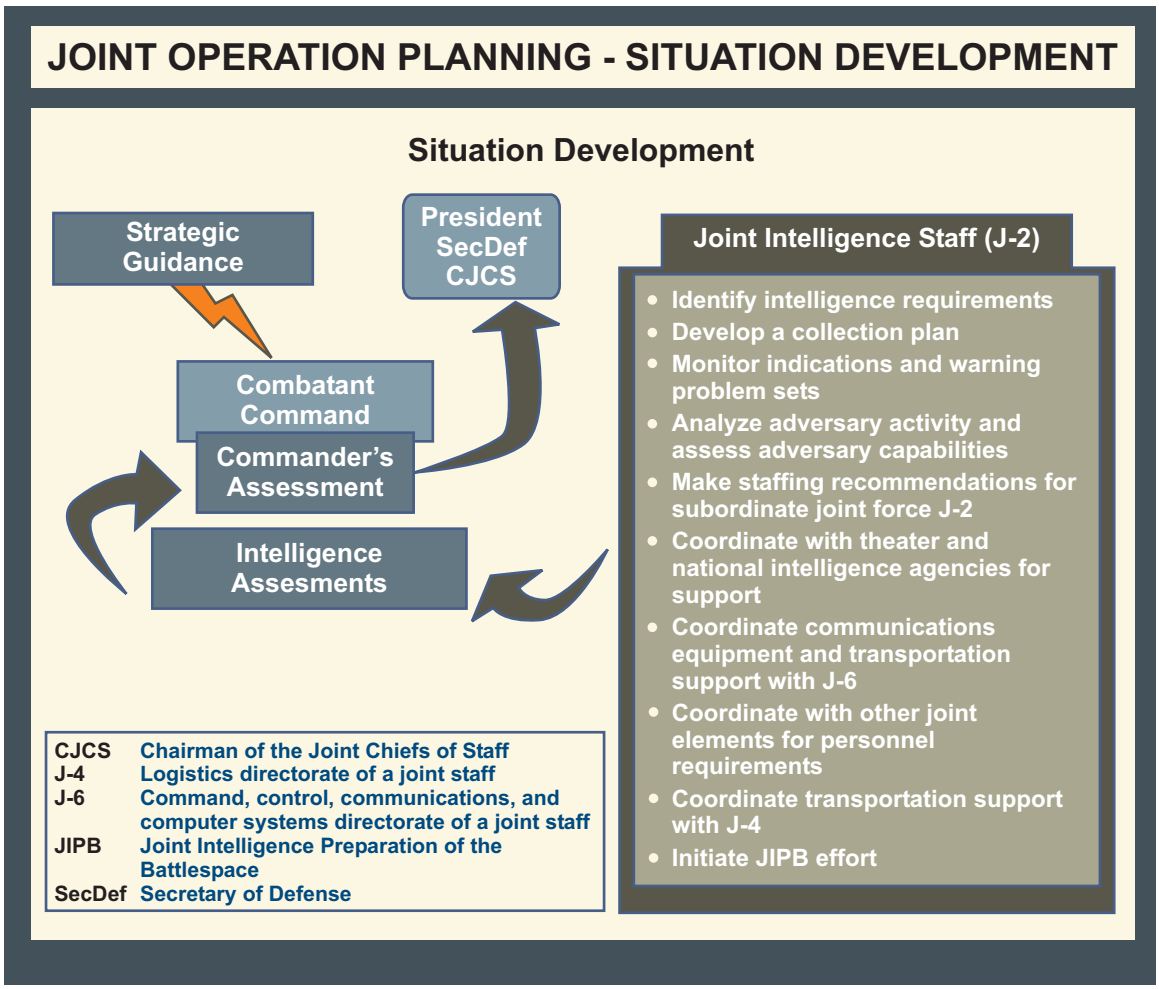


Figure IV-1. Joint Operation Planning — Situation Development

with the best intelligence possible throughout the operation. The J-2 staff should review all applicable joint intelligence lessons learned and initiate the JIPB effort.

c. **Crisis Assessment.** Intelligence facilitates the preparation of the combatant commander's assessment, which is submitted to the Secretary of Defense and Chairman of the Joint Chiefs of Staff for review. The National Security Council (NSC), President and/or Secretary of Defense, and the JCS analyze the combatant commander's assessment and determine whether a military option should be prepared. This activity requires increased intelligence gathering, JIPB, and analysis, particularly with respect to potential strategic lift destinations and available foreign infrastructure. Therefore, the combatant command J-2 must work closely with national agencies to help define and then answer the emerging intelligence requirements of the senior leadership and answer the commander's PIRs (see Figure IV-2). The analysis of the combatant commander's assessment results in a decision by the President or Secretary of Defense to return to the pre-crisis state or to have military options developed for consideration and possible use. The decision by the President or Secretary of Defense provides strategic guidance for joint operation planning and may include specific guidance on the COAs to be developed. The responsibilities of the theater J-2 during situation development include:

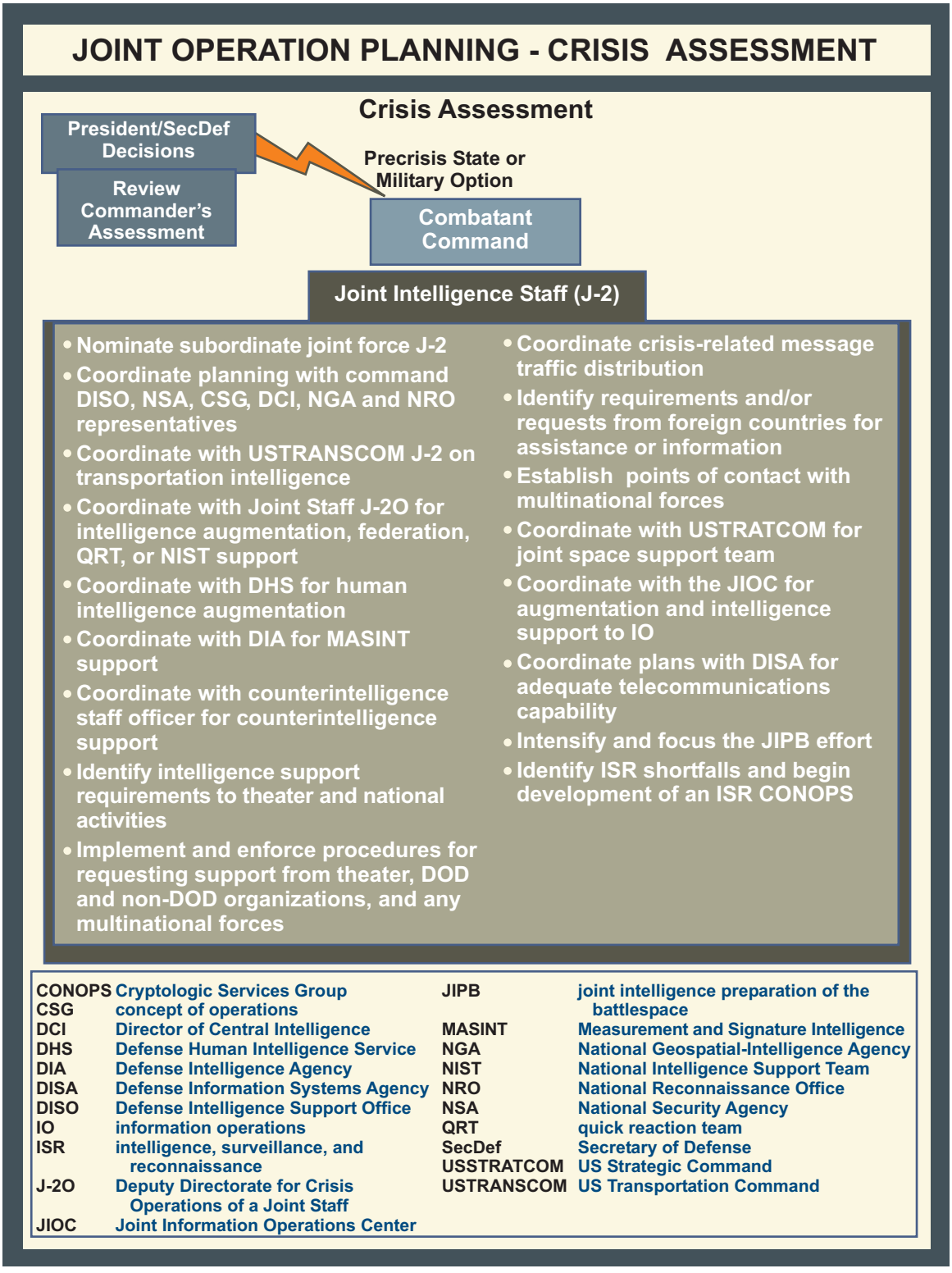


Figure IV-2. Joint Operation Planning — Crisis Assessment

(1) As required, the J-2 should nominate a subordinate joint force J-2 for consideration by the subordinate JFC. Once identified, the subordinate joint force J-2 then needs to coordinate with the combatant command J-2 and begin organizing, equipping, and preparing for the impending mission. JP 1-0, *Doctrine for Personnel Support to Joint Operations*, provides doctrine on assigning personnel to meet combatant command and UN mission-related temporary duty assignments. Procedures include the combatant commander requesting intelligence personnel from the Joint Staff Manpower and Personnel Officer (J-1); the Director Military Intelligence and the Military Intelligence Board validating and recommending resourcing of the requirement; and meeting crisis requirements by assigning higher priority to requests for personnel. Reserves should be included in sustainment plans for long term joint force requirements.

(2) Coordinate with the combatant command DISO, and NSA/CSS, CSG, DCI, NGA, and NRO representatives to ensure that they are informed of a Presidential or Secretary of Defense decision and the CJCS's planning guidance directive.

(3) Coordinate with United States Transportation Command (USTRANSCOM) J-2 and JIC to ensure that required intelligence is provided to transportation planners. Coordinate with the J-4 and J-5 to determine the effect that transportation infrastructure status has on deployment planning for intelligence assets as early as possible in the planning effort.

(4) Coordinate with Joint Staff J-2O for intelligence augmentation, federation, QRT, or NIST support, if required. Be prepared to define the supported command, required team capabilities, number of teams required, geographic locations for deployment, and required deployment data.

(5) Coordinate with DHS for HUMINT augmentation. The command HSE is the conduit for HUMINT support coordination.

(6) Coordinate with DIA for MASINT support or augmentation. During non-duty hours contact DIA's MOCC.

(7) Coordinate with the counterintelligence staff officer (CISO) for initiation of critical predeployment activities, realignment of ongoing CI support, and augmentation from the Services.

(8) Notify all relevant theater and national activities of possible requirements for intelligence collection, production, processing, reporting, and/or dissemination assistance. Be prepared to state what assistance will be required, when it will be needed, and the duration of the requirement.

(9) Implement and enforce procedures for requesting support from theater, DOD and non-DOD organizations, and any multinational forces. Identify problems and sensitivities. Requests for sensitive support will be coordinated with and processed through J-3 operations channels IAW DODD S-5210.36, *Provision of DOD Sensitive Support to DOD Components and Other Departments and Agencies of the US Government*. All intelligence and other government agencies affected by or involved with sensitive support must also be kept informed.

(10) Place the combatant command J-2 on distribution for all crisis-related traffic generated by theater and national intelligence activities. Ensure that the combatant command J-2 has access to any compartmented message traffic. Review the command's SIIs, which are key to receipt of intelligence traffic and special requests for documents. Coordinate changes with DIA.

(11) Identify, in coordination with the J-3 and J-4, requirements and/or requests from foreign countries for assistance or information. If required, begin coordinating requests for foreign disclosure and/or release with DIA. Consult with the Joint Staff J-2 on the status of possible multinational actions and associated intelligence support requirements.

(12) Establish POCs with multinational forces. Determine if any special language or translation requirements exist which will necessitate linguist augmentation.

(13) Coordinate with USSTRATCOM for joint space support team (JSST) augmentation. USSTRATCOM will deploy task-organized JSSTs to the supported command to provide space-derived intelligence, and ensure that support is provided. Information required includes: specific support teams, where they will be located, what is required, and approximately when the teams are required to be in place.

(14) Coordinate with the JIOC for augmentation and intelligence support to IO.

(15) Coordinate plans in advance with DISA to ensure adequate telecommunications capability is provisioned in the intended operational area.

(16) Intensify and focus the combatant command's JIPB effort.

(17) Identify ISR asset shortfalls, and in conjunction with J-3, begin development of an ISR CONOPS for the optimal use of ISR assets and requested resources.

d. **COA Development**

(1) **COA development begins with a Presidential or Secretary of Defense decision or CJCS planning directive to develop military options in response to a given situation, and may include a CJCS warning order activating a designated JTF.** This directive and required actions are described in JP 5-0, *Doctrine for Planning Joint Operations*, and JP 5-00.2, *Joint Task Force Planning Guidance and Procedures*.

(2) During COA development, the supported commander identifies and analyzes appropriate COA and prepares a commander's estimate, to include an intelligence estimate (see Figure IV-3). COA development ends with submission of the supported commander's estimate to the Chairman of the Joint Chiefs of Staff for review, approval or modification. The Chairman of the Joint Chiefs of Staff prepares recommendations and advice for the President or Secretary of Defense regarding the COA presented in the commander's estimate.

Figure IV-3. Joint Operation Planning — Course of Action Development

(a) The intelligence staff supports COA development by collecting and analyzing all available information on the adversary, terrain, geography (geospatial), forecast METOC conditions, and other features of the battlespace to produce an intelligence estimate. See Appendix D, "Intelligence Estimate," for an example of the intelligence estimate format. Through the JIPB process, the J-2 staff determines potential adversary COAs and identifies the adversary's most likely and most dangerous COAs. The J-2 staff also serves as an integral part of a "red team cell" for the purpose of wargaming alternative friendly force COAs.

(b) Key COA development actions of the combatant command J-2 in coordination with or as requested by subordinate JTF J-2, are as follows:

1. Ensure the supported commander receives all the intelligence support needed from the command J-2 to develop the COA for the commander's estimate. Key to this is the timely preparation of the intelligence estimate (see Appendix D, "Intelligence Estimate," for a sample intelligence estimate format).

2. Brief the subordinate joint force J-2 personnel on mission objectives and guidance contained in the warning order.

3. Evaluate systems, supply, and equipment requirements associated with each COA. Mobility planning requires a decision on what to ship to the subordinate joint force location along with the required delivery date and priority in the TPFDD. Identify external theater and/or national intelligence and communications systems required to support subordinate joint force operations. Include this information in the commander's estimate.

4. Brief combatant command J-2 staff on the warning order and advise them of potential requirements for augmentation (personnel and/or equipment).

5. Prepare general collection priorities and requirements for subordinate joint force support and coordinate requirements with the combatant command J-2. The combatant command J-2 coordinates with national collection authorities at DIA, NSA, NGA, and CIA to notify them of impending requirements and determine availability of resources.

6. If required, request tactical exploitation of national capabilities (TENCAP) support. The J-2 can request additional TENCAP support, including prototype and demonstration systems, through Service TENCAP offices. If required, additional support may be requested from NRO.

7. Review facility security requirements. Prepare request(s) for accreditation of facilities, if required. Refer to Appendix E, "Security," for detailed instructions regarding SCIF accreditation.

8. Continue to review requirements for systems interoperability and/or interconnectivity, and report on possible multi-Service and/or multinational interoperability problems. Coordinate with the agencies and organizations involved.

9. Continue to coordinate requests for foreign disclosure and/or release issues with DIA, as appropriate. Obtain waivers if required.

10. Establish new DMS addressee lists for receiving and sending pertinent subordinate joint force J-2 message traffic.

11. Eliminate duplicative intelligence and avoid unnecessary redundancy in the re-transmittal or rebroadcast of intelligence information.

12. Identify combatant command, Service, or subordinate joint force J-2 requirements for communications support. Coordinate all requirements for systems and frequencies with the combatant command and subordinate joint force J-6. Forward requests for national-level communications support through the combatant command J-6 to the Joint Staff J-2 for validation and the Joint Staff J-6 for tasking.

13. Coordinate a joint restricted frequency list with the command J-2, J-6, and NSA.

14. Report major capability limiting factors (shortfalls) in any area for possible inclusion in the commander's estimate.

15. Request a current profile on disease and environmental hazards from DIA's AFMIC.

16. Locate all TIM sites and estimate their potential hazard.

17. Review the checklist found in JP 5-00.2, *Joint Task Force Planning Guidance and Procedures*, Appendix C, Annex B. This checklist contains selected questions the J-2 should consider.

(c) Up to this point, planning for subordinate joint force J-2 operations has been centered in the combatant command J-2. However, during COA development, the subordinate joint force J-2 staff begins forming a JISE and assumes leadership for J-2 CAP. A JISE will provide the JFC with complete information and intelligence on the air, space, ground, and maritime adversary situation. Subordinate joint force J-2 considerations include the following:

1. The supported combatant command forms a subordinate joint force, with planning centering on the issues of mobilization and sustainability for the joint force. J-2 requirements for transportation are entered into JOPES during this phase. Input must include anticipated requirements for attachments such as NIST and augmentation to the HOC and TFCICA.

2. The subordinate joint force J-2 should keep JOPES managers apprised of intelligence personnel and equipment movement requirements. The sequenced arrival of deployed J-2 personnel and materiel, including NIST assets, needs to be planned and coordinated early. POCs should be identified to work with the combatant command J-3 and/or J-4 as well as joint force J-3 and/or J-4 on J-2 movement requirements.

3. Requesting commands must logistically support the NIST and other external augmentation elements.

4. Formal requests for DISA support must be coordinated with the J-6.

5. The subordinate joint force J-2 and J-3 should analyze ISR capabilities relative to each COA and identify shortfalls that may require the deployment of additional ISR resources.

e. **Concept Development. CONOPS development is initiated after the President or Secretary of Defense approves a COA.** An alert order implements the Presidential or Secretary of Defense decision and contains sufficient detail to allow the JFC to conduct detailed planning. A CJCS planning order could be issued to initiate execution planning before the President or Secretary of Defense selects a COA. The supported combatant commander expands the approved COA into an executable CONOPS, which is reviewed and approved by the Chairman of the Joint Chiefs of Staff, and forms the basis for subsequent OPLAN development by the combatant command staff.

(1) During **CONOPS development**, the focus of the subordinate joint force J-2 planning effort shifts to the COA selected by the President or Secretary of Defense (see Figure IV-4). In addition, the subordinate joint force J-2 will:

(a) Coordinate with Joint Staff J-2O via record message for NISTs, QRTs, federation, augmentation, and all other external support from national intelligence agencies that involves personnel and/or equipment. Submit all support requests to Joint Staff J-2 via the combatant commander for validation and subsequent action. Follow-up on any requests submitted earlier in the planning process.

(b) Ensure that all subordinate joint force J-2 personnel understand the organizational structures, command, support and multinational relationships established for the mission. Joint force J-2 personnel should be briefed on key C2 relationships affecting their specific responsibilities.

(c) Finalize communications support for the subordinate joint force J-2. Develop back-up procedures, in coordination with the J-6, for maintaining support to customers if primary communications are lost.

(d) Prepare and publish the PIR pertinent to the upcoming mission. PIR are formally published in the OPLAN.

(e) Publish and distribute the CONOPS for the subordinate joint force JISE. The JISE evolves and is sized to meet the specific crisis or contingency with an intelligence structure that matches the mission.

(f) Submit DMS address lists to J-6 for sending and receiving message traffic.

(g) Ensure that requests for theater and national augmentation (personnel and equipment) are formally submitted and track responses. Coordinate with J-1 to ensure that logistic preparations for locating and housing augmentees are underway.

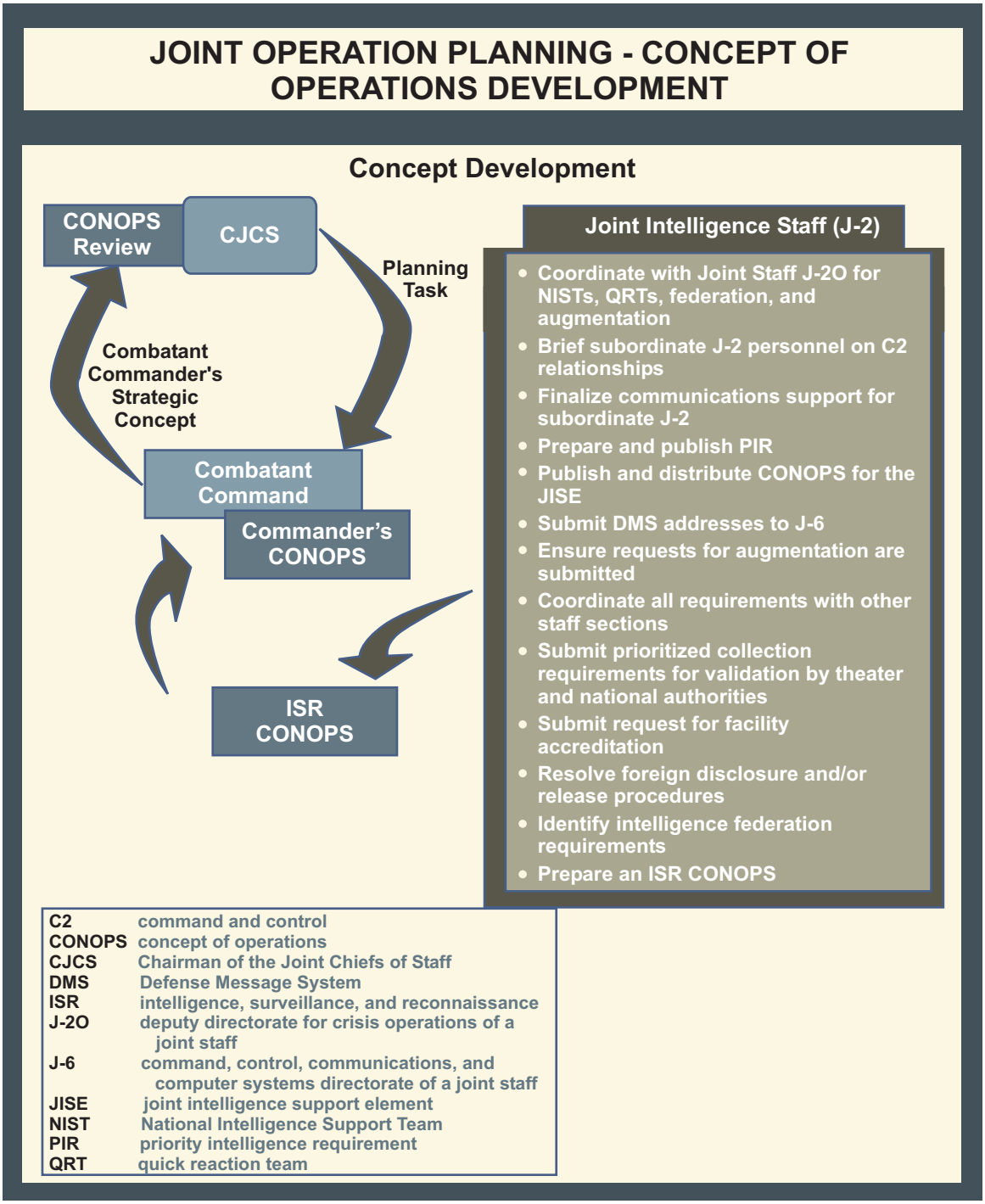


Figure IV-4. Joint Operation Planning — Concept of Operations Development

(h) Coordinate final personnel, systems, supply, equipment and communications security materials requirements with subordinate joint force J-1, J-3, J-4, J-5, and J-6, and submit them IAW command procedures for inclusion in JOPES and the TPFDD.

(i) Submit prioritized collection requirements for validation by theater and national authorities. Inform combatant command ISR planners and schedulers of required start date for theater-based ISR support.

(j) Submit and track the request for facility accreditation to ensure that a decision is made.

(k) Resolve foreign disclosure and/or release procedures. Inform all subordinate joint force personnel of procedures for handling disclosure and/or release of intelligence to foreign nationals. Requirements and procedures for sharing intelligence with multinational forces must be finalized and specific products to be shared must be identified in the JISE CONOPS and in the OPORD. Coordinate with the Joint Staff J-2 for support being provided to multinational forces through the UN, NATO, or other international organizations.

(l) Identify intelligence federation requirements and develop an intelligence federation plan.

(m) In conjunction with J-3, prepare an ISR CONOPS to optimize the utilization of all available and requested ISR assets and resources.

(2) The approved combatant commander's CONOPS provides the basis for plan development by the combatant commander's staff.

f. **Plan Development**

(1) Deliberate planning and CAP for any particular joint operation are interrelated by the degree to which deliberate planning has been able to anticipate and prepare for the crisis. Every crisis situation cannot be anticipated, but detailed analysis and coordination accomplished during the deliberate planning period may greatly expedite effective decision making and execution planning during crises and unanticipated contingencies. Therefore, **joint intelligence support for CAP should always begin with a thorough exploitation of relevant deliberate plans**. The planning component of the joint operation planning process includes all of the activities that must be accomplished to prepare for an anticipated operation. It includes those activities required to prepare for the mobilization, deployment, employment, and sustainment of forces leading up to, but not including, the actual movement of those forces.

(2) During plan development, the intelligence staffs are responsible for developing the Intelligence Annex and appendices to the basic OPLAN. Additionally, if required, the intelligence staff develops the Geospatial Information and Services (GI&S) Annex to the OPLAN. Intelligence staffs must also identify intelligence support force and sustainment requirements and identify intelligence shortfalls throughout the planning process for incorporation into the OPLAN. Intelligence assets must be included in the time-phased force and deployment list (TPFDL) to ensure proper movement of critical personnel and equipment. The J-2 must coordinate with the combatant command J-6 to ensure intelligence communications requirements are incorporated in Annex K of the combatant command's OPLAN (see Figure IV-5).

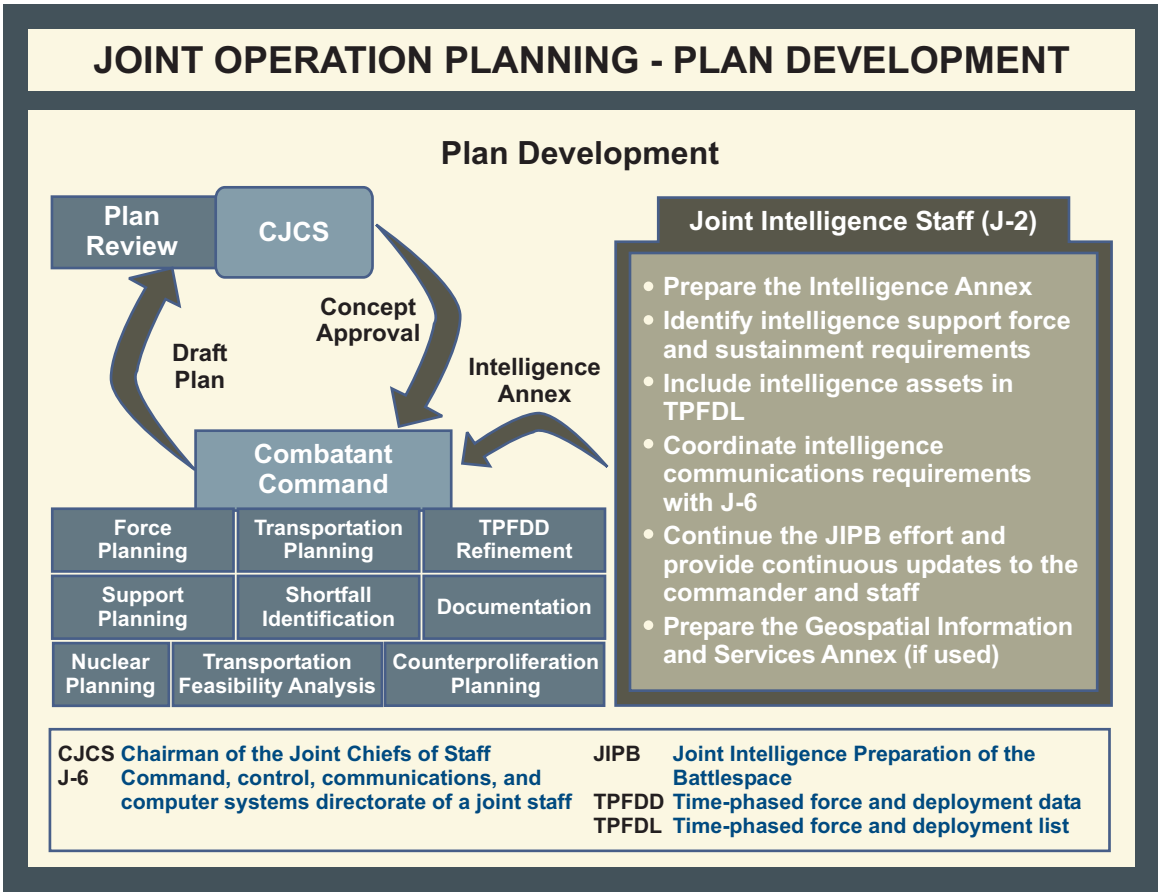


Figure IV-5. Joint Operation Planning — Plan Development

(3) Appropriate subordinate joint force J-2 planning actions during this period include the following:

(a) Brief the subordinate joint force J-2 staff, DISO, NCR, CSG, HSE, MASLO, CISO, and the NRO, NGA and CIA representatives on the execute order.

(b) Review Appendix C in JP 5-00.2, *Joint Task Force Planning Guidance and Procedures*, and Appendix C of this publication, "Representative Intelligence Requirements," which list general intelligence responsibilities associated with a subordinate joint force. Develop the OPORD's Annex B (Intelligence) and Annex M (Geospatial Information and Services) according to CJCSM 3122.04, *Joint Operation Planning and Execution System, Vol II: (Supplemental Planning and Execution Formats and Guidance)*.

(c) Ensure that all personnel have reviewed and understand the "JISE" operations concept. Ensure that C4 systems relationships have been defined for support to major component forces of the subordinate joint force.

(d) Ensure that JISE procedures affecting highly time-sensitive and mission-critical operations and/or intelligence interfaces are thoroughly practiced and deconflicted. Highly time-

sensitive interfaces usually include SOF operations, targeting, WMD detection, and the joint search and rescue center. Other interfaces may be created depending upon how the subordinate joint force is constituted. Requests for SOF and other specialized time-sensitive operational support will be coordinated through J-3 operations and may require special category communications procedures.

(e) Apprise the supported commander of the current status of intelligence and CI capabilities and limitations.

(f) Enumerate changes, if any, in the adversary's situation that could require a change in the COA selected.

(g) Request the activation of pre-planned crisis intelligence federation partnerships as required.

g. The **Chairman of the Joint Chiefs of Staff conducts a final review of OPLANs** submitted by the supported commander during plan review. This review evaluates the plan to determine whether taskings have been met and whether resources have been used effectively within the constraints of the JSCP apportionment guidance. The Chairman of the Joint Chiefs of Staff monitors planning activities, resolves shortfalls when required, and reviews the supported commander's OPLAN for feasibility, adequacy, acceptability, and compliance with joint doctrine. The Joint Staff J-2, Services, and intelligence combat support agencies (DIA, NGA, NSA) review the intelligence and GI&S annexes for the Chairman of the Joint Chiefs of Staff (see Figure IV-6).

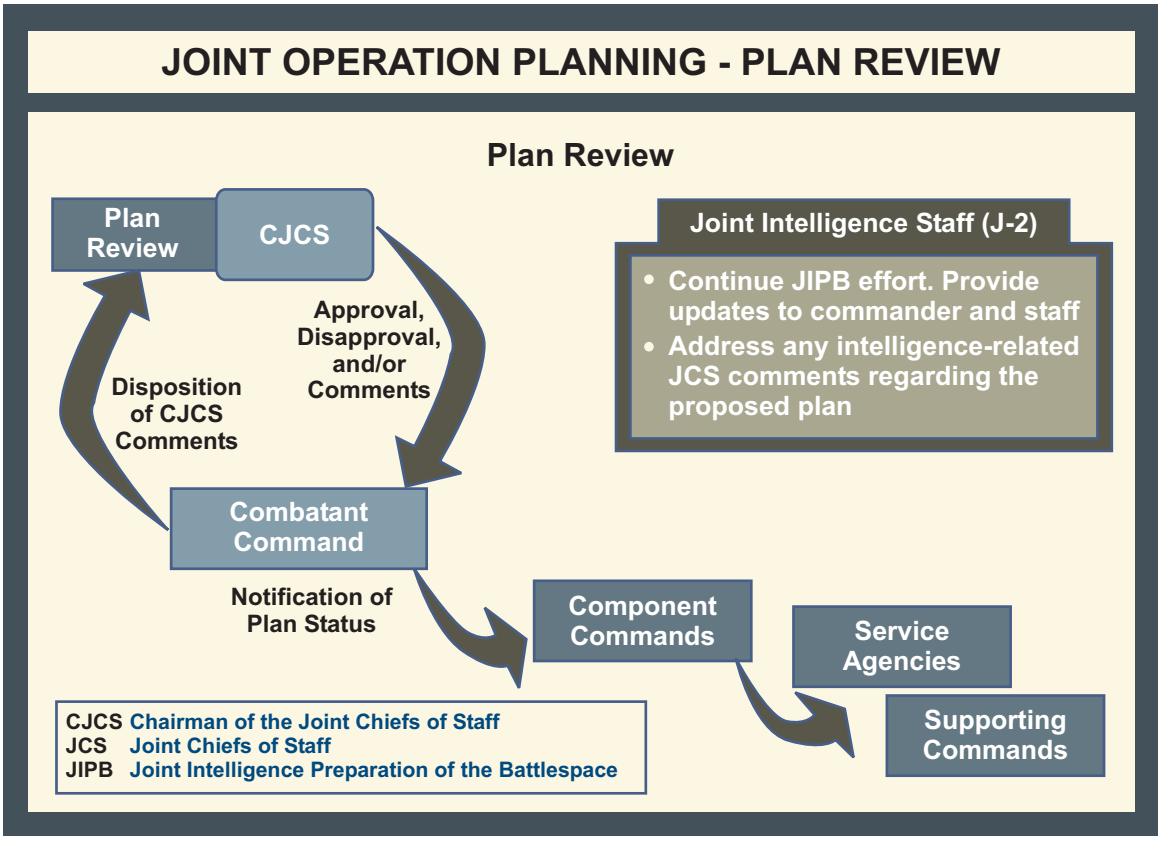


Figure IV-6. Joint Operation Planning — Plan Review

h. **Supporting Plan Development. Supporting plans are developed** to address mobilization, deployment, employment, sustainment, and redeployment of forces and resources in support of the concept described in the supported commander's approved plan. The intelligence combat support agencies (DIA, NSA, NGA) may be tasked by the combatant command to develop a supporting plan. The Chairman of the Joint Chiefs of Staff may be asked to resolve critical issues, including use of intelligence personnel and assets, that arise during the review of supporting plans. The Joint Staff may review any supporting plan on behalf of the Chairman of the Joint Chiefs of Staff (see Figure IV-7).

i. **Execution. If the President or Secretary of Defense decide to execute the selected COA, the Chairman of the Joint Chiefs of Staff issues an execute order.** The execute order directs the deployment and employment of forces, defines the timing for initiation of operations, and conveys guidance not provided in earlier joint operation planning orders and instructions. The execution portion of joint operation planning continues until the crisis or mission ends and force redeployment has been completed. If a crisis is prolonged, the process may be repeated continuously as circumstances change and missions are revised. If the crisis expands to major conflict or war, CAP will evolve into and be absorbed within the larger context of implementation planning for the conduct of the war. The subordinate joint force J-2 provides intelligence critical to current and future operations, planning, targeting, and force protection. Collection, analysis and reporting must answer the commander's PIRs and provide predictive intelligence and assessments, with emphasis on intelligence involving the movement and disposition of hostile forces. Adversary movements of

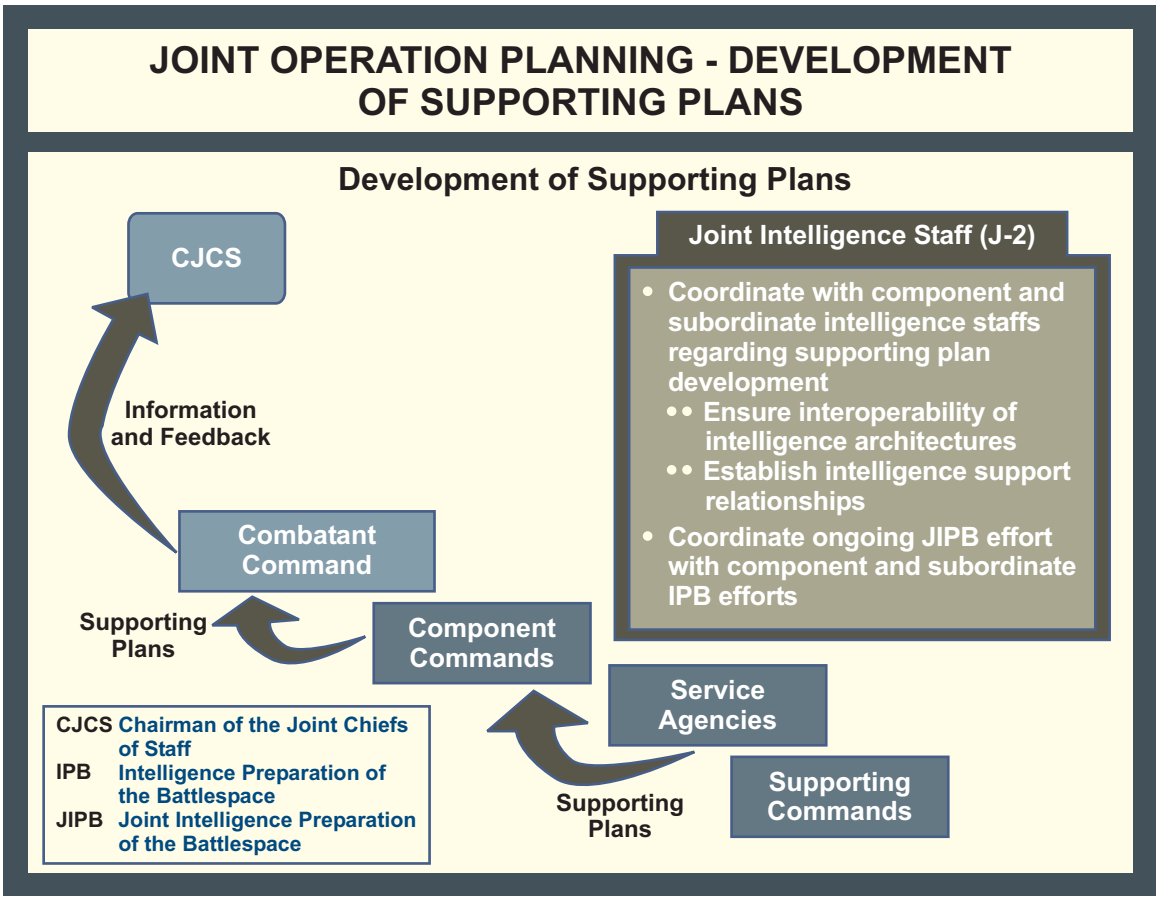


Figure IV-7. Joint Operation Planning — Development of Supporting Plans

interest to SOF are among the top joint force reporting priorities during execution. The supported combatant command J-2 must be prepared to assume this reporting responsibility until the subordinate joint force J-2 has reached full operational status at the deployed location (see Figure IV-8).

3. Campaign Planning

The theater campaign plan embodies the combatant commander's vision of related major operations required to attain strategic objectives. Campaign planning is appropriate when military operations exceed the scope of a single major operation. It encompasses both the deliberate and crisis action planning processes. The campaign plan focuses on the adversary's COGs; the integrated employment of land, sea, air, space, and SOF assets; and the end state to be achieved. **Intelligence efforts in support of the campaign plan, including the intelligence annexes, focus on identifying any adversary forces and capabilities in the AOR and/or JOA and the adversary's strategic and operational COGs** (see Figure IV-9).

4. Planning for Multinational Operations

In most multinational operations, the JFC will be required to share intelligence with foreign military forces and to coordinate receiving intelligence from those forces. In some circumstances, the JFC will need to seek authority to go outside the usual politico-military channels to provide information to nongovernmental and international organizations. **Unique intelligence policy and dissemination criteria will have to be tailored to each multinational operation.**

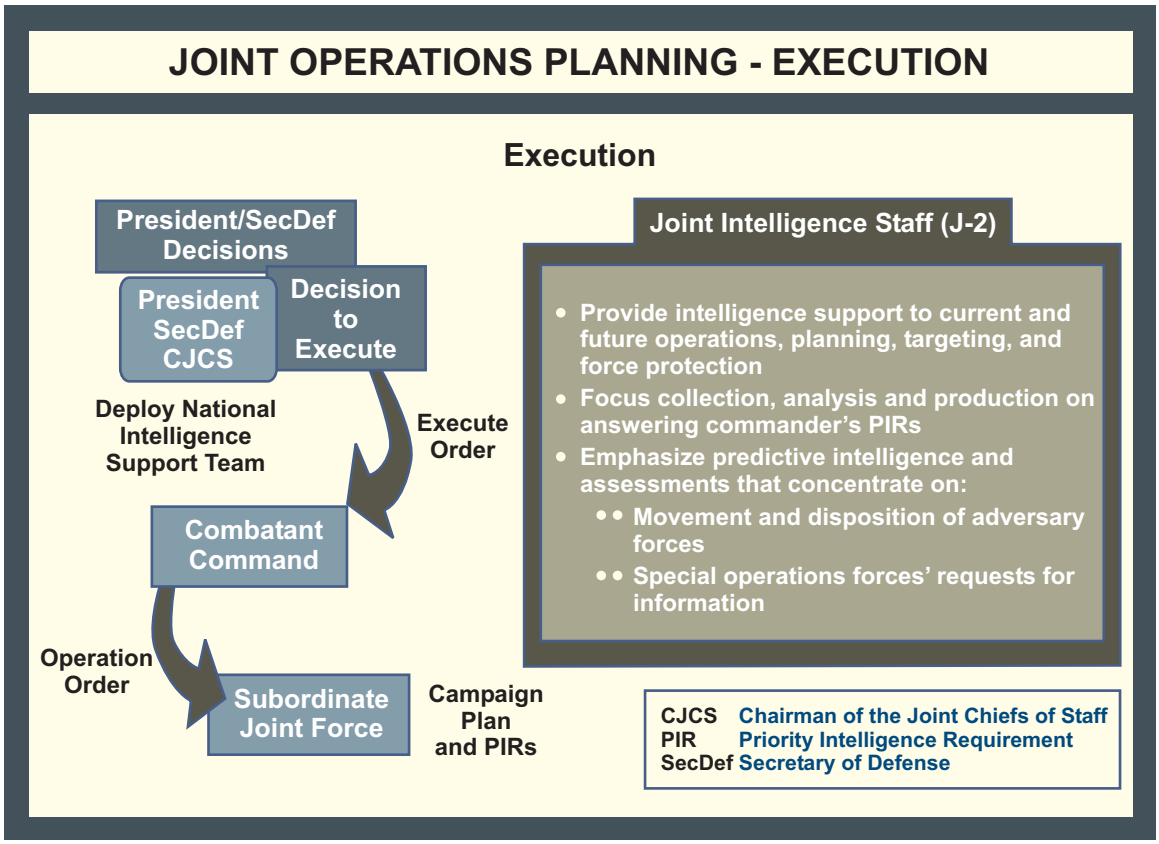


Figure IV-8. Joint Operations Planning — Execution

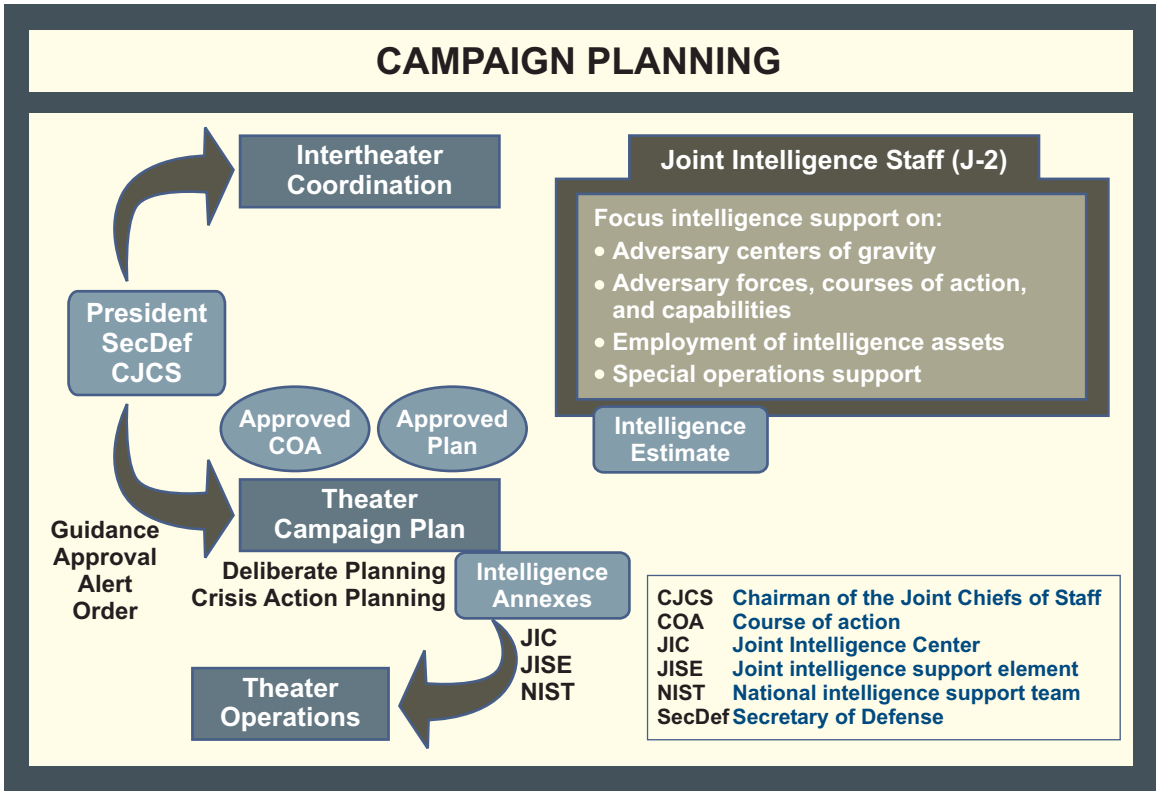


Figure IV-9. Campaign Planning

a. **Intelligence Principles for Multinational Operations.** In some multinational operations or campaigns, JFCs will be able to use existing international standardization agreements (STANAGs) (e.g., NATO STANAGs) as a basis for establishing rules and policies for conducting joint intelligence operations. Since each multinational operation will be unique, such agreements may have to be modified or amended based on the situation. A JFC participating in a coalition or alliance must tailor the policy and procedures for that particular operation based on theater guidance and national policy as contained in National Disclosure Policy (NDP) 1, *National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations*. NDP 1 provides policy and procedures in the form of specific disclosure criteria and limitations, definition of terms, release arrangements, and other guidance. The disclosure of classified information is never automatic. Any disclosure must be consistent with US national policy and US military objectives, be done with security assurances in place, present a clearly defined US advantage, and be limited to only necessary information. The general principles outlined in Figure IV-10 provide a starting point for creating the necessary policy and procedures.

(1) **Maintain Unity of Effort.** Intelligence personnel of each nation need to view the threat from multinational as well as national perspectives. A threat to one element of an alliance or coalition by the common adversary must be considered a threat to all alliance or coalition elements.

(2) **Make Adjustments**

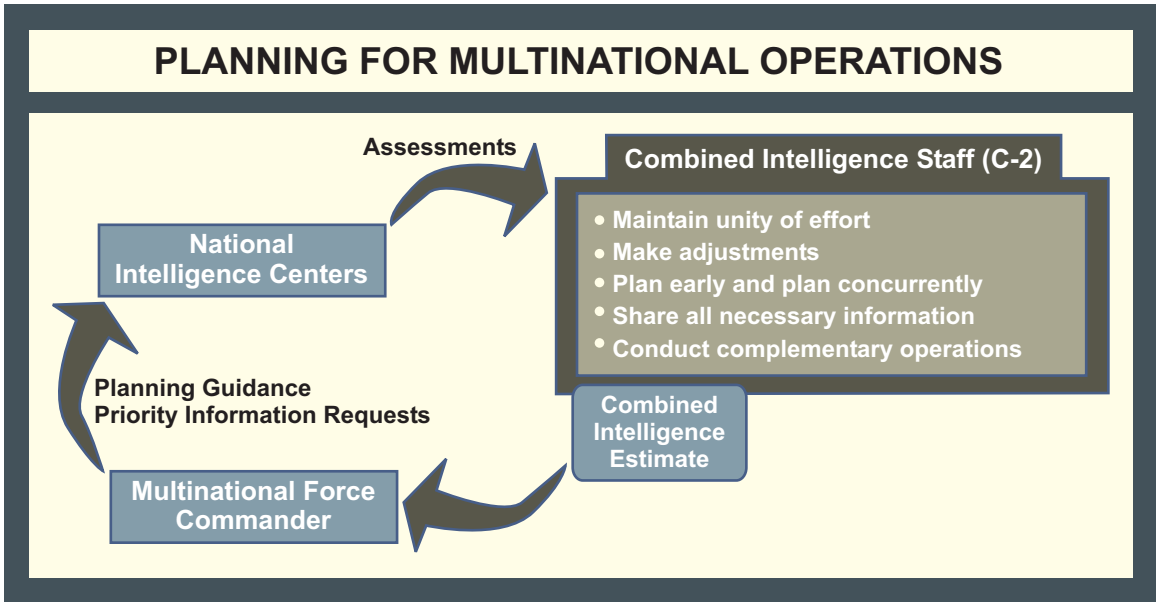


Figure IV-10. Planning for Multinational Operations

(a) There will be differences in intelligence doctrine and procedures among the coalition partners. A key to effective multinational intelligence is readiness, beginning with the highest levels of command, to make the adjustments required to resolve significant differences.

(b) Major differences may include how intelligence is provided to the commander (jointly or individual Services or agencies), procedures for sharing information among intelligence agencies, and the degree of security afforded by different communications systems and procedures. Administrative differences that need to be addressed may include classification levels, personnel security clearance standards, requirements for access to sensitive intelligence, and translation requirements.

(3) **Plan Early and Plan Concurrently.** JFCs need to determine what intelligence may be shared with the forces of other nations early in the planning process. NATO and the United States-Republic of Korea Combined Forces Command have developed and exercised intelligence policies and procedures that provide examples of how multinational planning can be done in advance.

(4) **Share All Necessary Information**

(a) Multinational partners should share all relevant and pertinent intelligence about the situation and adversary consistent with NDP and theater guidance. However, information about intelligence sources and methods should not be shared with multinational partners until approved by the appropriate national-level agency.

(b) Force protection is a mission inherent to any commander, and intelligence and CI support to that mission is critical. Every effort must be made to share any data that could impact on the commander's force protection mission.

(c) When information relating to a particular source cannot be shared, the intelligence derived from that source should still be provided to other multinational partners. The J-2 must establish procedures for separating intelligence from sources and methods. Whenever possible, intelligence production agencies should print highly classified reports in such a manner that compartmented information is separated from intelligence that can be widely disseminated by a "tear line" (the J-2, G-2, and/or S-2 keeps information above the tear line and disseminates the intelligence below). Having intelligence production agencies use such tear lines will greatly facilitate intelligence sharing.

(d) The joint force J-2 must obtain the necessary foreign disclosure authorization from DIA as soon as possible. J-2 personnel must be knowledgeable of the specific foreign disclosure policy, procedures, and regulations for the operation. The efficient flow of intelligence will be enhanced by the assignment of personnel knowledgeable of foreign disclosure.

Appendix E, "Security," contains a detailed discussion of sanitization and foreign disclosure procedures.

(5) **Conduct Complementary Operations**

(a) The intelligence efforts of nations participating in multinational operations must be complementary. Each nation will have intelligence system strengths and limitations, and unique and valuable capabilities that should be used to offset shortfalls in US intelligence resources. Host-nation security services' capabilities, for example, will contribute significantly to force protection. Furthermore, planning with friendly nations to fill shortfalls, especially linguists requirements, may help overcome such limitations. Additionally, the ISR assets of participating nations (especially high demand airborne ISR platforms) should be fully integrated into the multinational force's intelligence collection plan.

(b) All intelligence resources and capabilities should be made available for application to the whole of the intelligence problem. Establishing a multinational collection management element is essential for planning and coordinating multinational collection operations.

b. **Multinational Intelligence Architecture.** An intelligence operational architecture must be planned and established for every multinational operation to help unite the national intelligence cells of participating coalition members in a common effort. Information sharing should be facilitated by establishing a coalition local area network using systems such as Linked Operations-Intelligence Centers Europe (LOCE) and Combined Enterprise Regional Information Exchange System (CENTRIXS). These and other US and allied information sharing systems are discussed in greater detail in Chapter V, "Intelligence and the Global Information Grid." A notional multinational intelligence architecture is depicted in Figure IV-11 and provides a starting point from which a more detailed architecture can be developed.

(1) **A multinational intelligence center is necessary** for merging and prioritizing the intelligence requirements from each participating nation and for acquiring and fusing the nations' intelligence contributions. The multinational intelligence center must include representatives from all nations participating in the multinational operation. Designating a single Director of Intelligence for the multinational command will greatly assist in resolving the inevitable differences among the multinational members.

(2) Critical to the multinational architecture is **developing a standardized methodology for disseminating and exchanging intelligence**. When possible, the methodology must be conceived and exercised as part of the multinational planning process before operations begin. The effectiveness of the methodology must be monitored and, when necessary, adapted during operations to meet changing circumstances.

(3) **Intelligence liaison is critical** between commands and among supporting and supported organizations. Liaison personnel are instrumental in resolving problems resulting from language barriers and cultural and operational differences that normally occur in multinational operations. Because of the inherent complexities associated with multinational operations, an aggressive liaison effort is critical to developing and maintaining unity of effort. A robust liaison effort with sufficient communications is particularly critical in the initial stages of planning and forming a coalition, particularly when the US intelligence network is not yet established.

(4) In addition, **US SOF may be assigned to coalition members' organizations** to conduct coalition support. These coalition support teams have the ability to receive and disseminate intelligence directly to and from their counterparts.

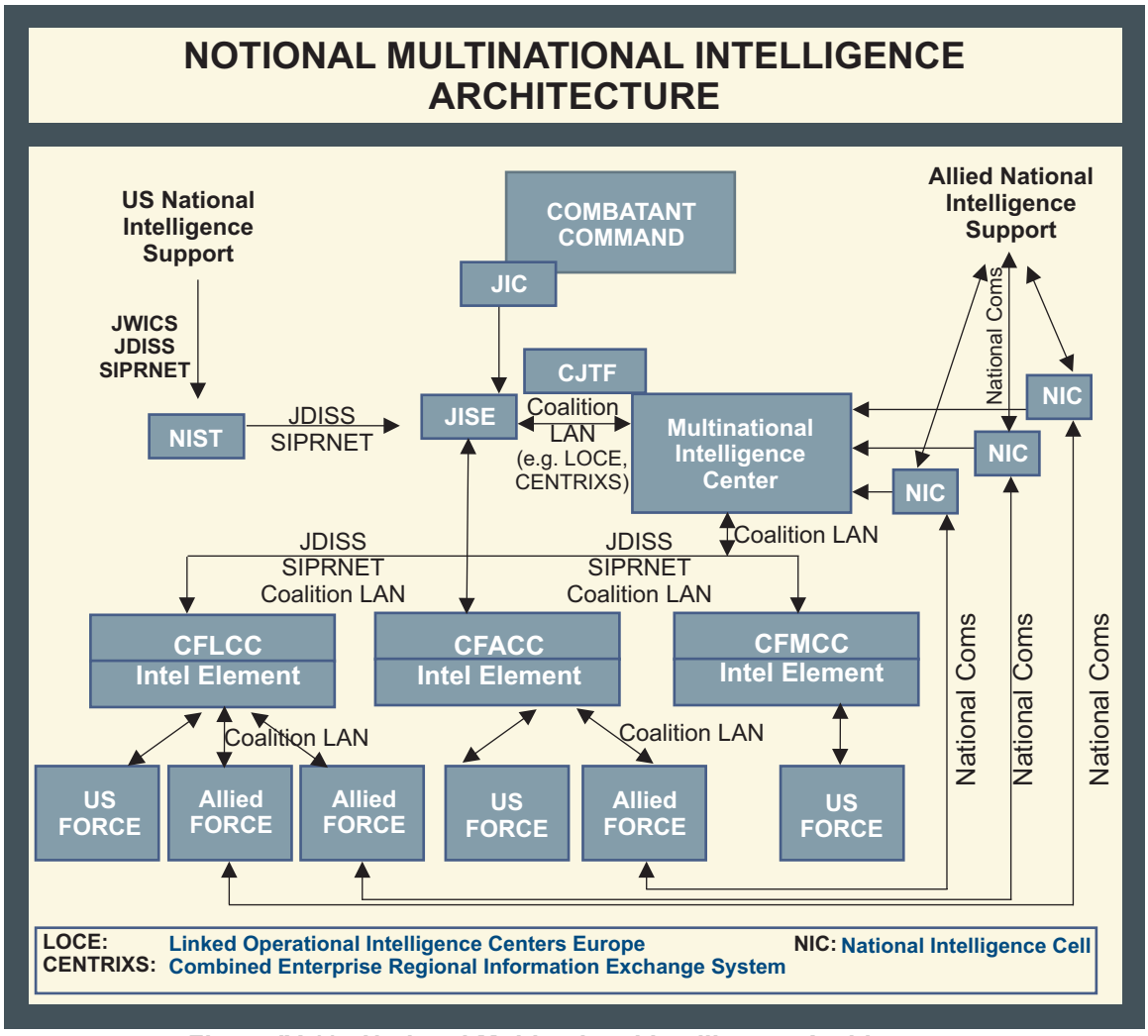


Figure IV-11. Notional Multinational Intelligence Architecture

(5) The multinational operational architecture portrayed in Figure IV-12 was established to support US and UN forces in Somalia as members of the UN Operations in Somalia (UNOSOM II) effort. Two levels of intelligence were established: Level 1 data could be shown to but not retained by coalition forces or the UN, while Level 2 data was cleared for release to the coalition and the UN. Level 1 intelligence remained within US-only channels, while Level 2 data flowed to the UNOSOM II information center in Mogadishu either from the UN HQ or via the US JISE.

(6) **In some situations there may be more than two levels of intelligence required.** For example, an operation involving a mixture of NATO and non-NATO forces could have "US Only," "Releasable to NATO," and "Releasable to Non-NATO" levels. The multinational force commander (MNFC) will play a major role in advising the national IC on the intelligence requirements for each of the coalition members. The MNFC will need to recommend what intelligence should be provided to each member.

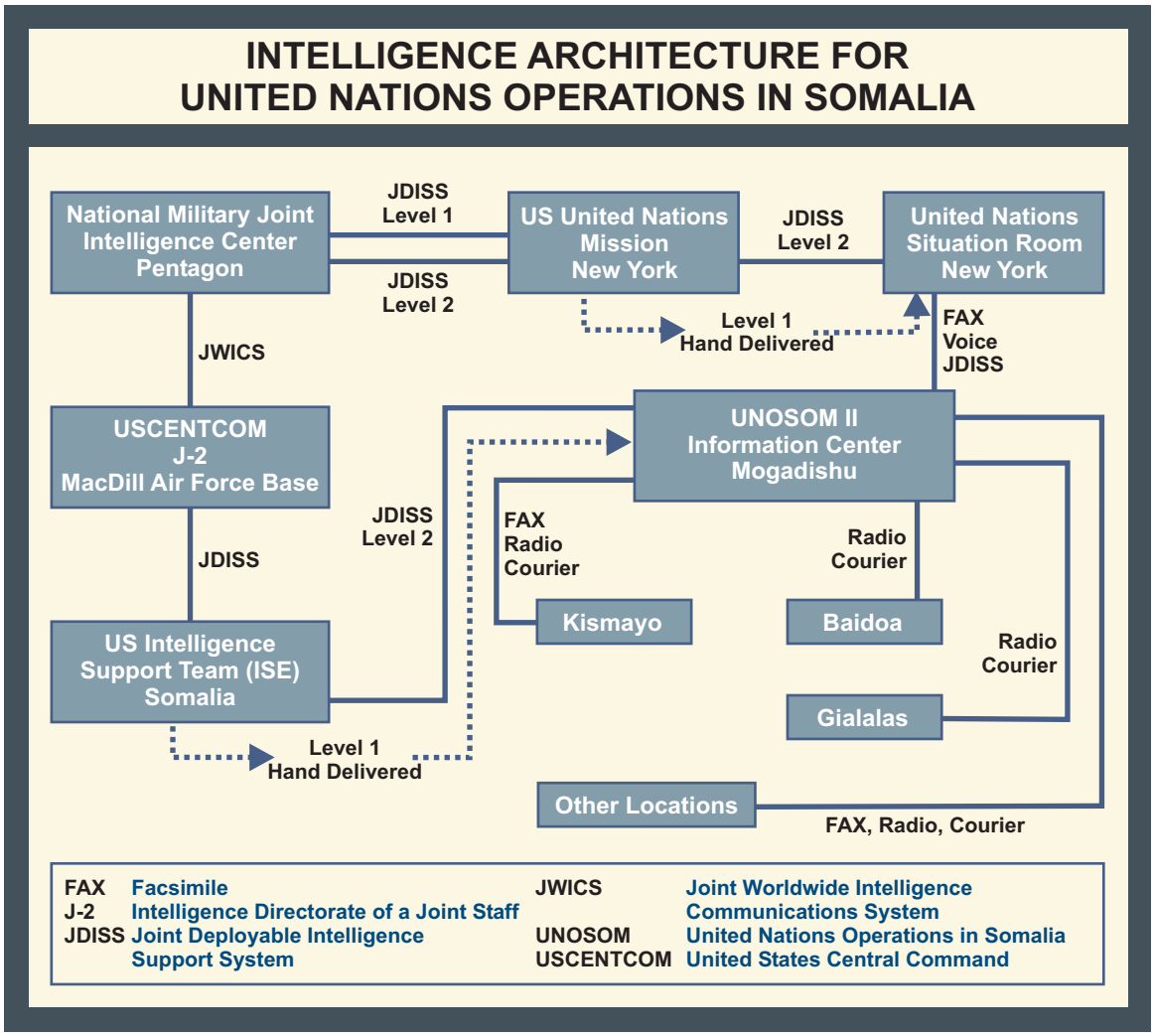


Figure IV-12. Intelligence Architecture for United Nations Operations in Somalia

(7) Figure IV-13 illustrates the intelligence structure established by USEUCOM for Operation JOINT ENDEAVOR in Bosnia-Herzegovina. In this situation, USEUCOM established national intelligence centers at each NATO HQ to provide intelligence support to both NATO and US forces. NISTs were deployed to ensure timely dissemination of intelligence from national intelligence agencies.

5. Conclusion

The time required to plan subordinate joint force J-2 support depends largely upon how much can be adapted from already existing deliberate plans and the total time required for the CAP process in a given situation. In some cases, events could cause planning to skip directly to the execution phase. To prepare for this eventuality, combatant command J-2s should create their own crisis planning checklists and exercise them. Appendix A, "Joint Force J-2 Quick Reaction Checklist," provides a starting point for checklist development.

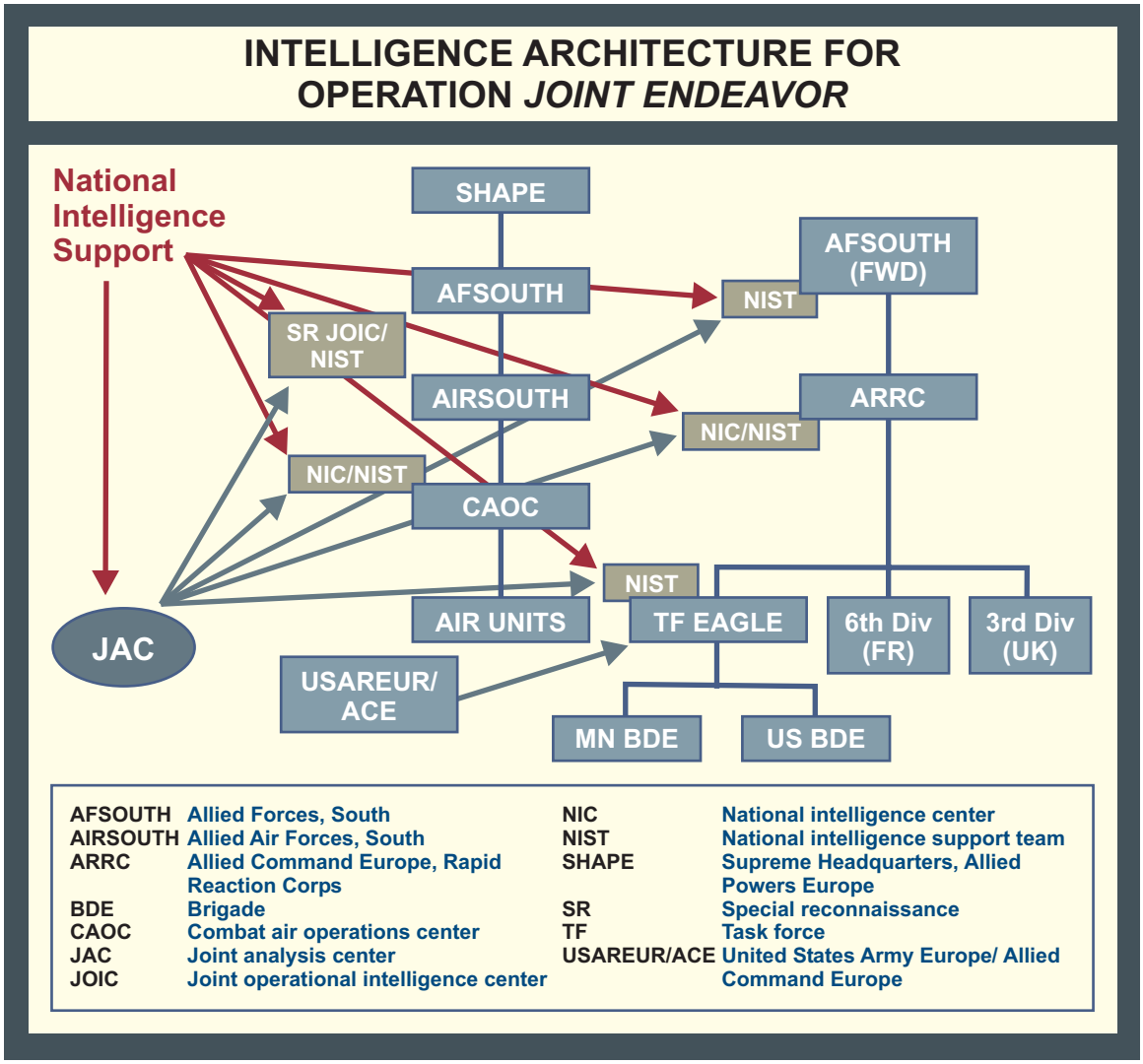


Figure IV-13. Intelligence Architecture for Operation JOINT ENDEAVOR

CHAPTER V
INTELLIGENCE AND THE GLOBAL INFORMATION GRID

"The success of any crisis deployment hinges on the existence of a reliable command and control system and of a flexible, reliable system for gathering, analyzing, and disseminating strategic and tactical intelligence."

General H. Norman Schwarzkopf, USA
Commander, United States Central Command
Operation DESERT STORM, 1991

1. Introduction

a. The GIG is the end-to-end integrated set of IT capabilities, associated processes and personnel for collecting, processing, storing, disseminating and managing information on demand to commanders, policy makers and support personnel in a globally interconnected environment. The GIG includes all DOD-owned and leased communications and computing systems, software, data, security services, and other associated services necessary to achieve information superiority. This environment supports all DOD and IC missions and functions (strategic, operational and tactical), in war and peace, at all operating locations (bases, posts, camps, stations, facilities, mobile platforms and deployed sites). The GIG provides interfaces to coalition, allied and non-DOD users and systems.

b. **The GIG integrates intelligence and operations information and schematics to provide a COP, facilitates interoperability between previously stovepiped Service information systems, and provides assured, secure, and tailorable information on demand to all appropriate users.** The modern communications and IT that make the GIG possible is undergoing continuous and rapid evolution. This technological dynamism affects all the various intelligence-related subarchitectures, systems, and applications resident in the GIG. This presents challenges regarding operator familiarization, the integration and interoperability of systems and networks, and the efficient utilization of available resources. These challenges can be overcome through dedicated, professional training, hands-on experience, and clear, workable, architectural standards.

(1) As discussed in JP 2-0, *Doctrine for Intelligence Support to Joint Operations*, the Director, DIA establishes capability and interoperability standards for joint and Service intelligence activities. The Director, DIA coordinates planning and programming of intelligence resources, including those for selected information systems, telecommunications, and survivability. DIA has established a standard communications architecture that supports joint intelligence operations. The combatant command then takes this standard "package" and, in coordination with DIA, builds a theater intelligence architecture based on the mission, combatant commander guidance, and command requirements.

(2) Developers, installers, and other information systems professionals must continuously improve the quality of their support to commanders by successfully creating and refining communications and information systems. However, technological development must

be realistically tempered by the limitations of fielded and deployed systems and of the consumers themselves.

2. Intelligence-Related Components of the Global Information Grid

The communications networks and information processing, storage, and management systems that comprise the GIG provide the basic framework for the timely transfer of data and information to support military operations. The GIG also provides the means for the timely dissemination of information and finished intelligence to commanders and other key decision makers, thereby facilitating information superiority. The GIG architecture implements common procedures, standards, and streamlined support, and continues to evolve. **The intelligence portion of the GIG is designed to provide an architecture that can be individually tailored to the specific needs of a joint force, ensures survivability and flexibility through distributed operations, and can be rapidly reconfigured to accommodate changing demands and responsibilities including facilitating relationships among federated intelligence partners.** This tailorable, distributed, and rapidly reconfigurable joint architecture provides all relevant available battlespace information to the user in the form of a COP. Within the GIG, the Department of Defense Intelligence Information System (DODIIS) is the aggregation of personnel, procedures, equipment, computer programs, and supporting communications of the military IC. DODIIS defines the standards for intelligence system and application interoperability. The system concept provides an integrated strategic, operational, and tactical user environment for performing identical intelligence support functions on compatible systems. DODIIS provides a robust and flexible intelligence capability for subordinate joint forces as long as supporting communications lines are available. DODIIS tools support the movement of intelligence between DIA, the combatant commands, the Services, and other intelligence production and customer activities worldwide. This program includes hardcopy products, digital or "softcopy" products, on-line access to databases, the ability to "push" or "pull" files of information between producers and consumers, CD-ROM storage, document imaging, electronic publishing, and networked (via internal local area networks [LANs] or JWICS) corporate mass storage devices which contain large volumes of digitized intelligence information. DODIIS encompasses the GIG components depicted in Figure V-1.

a. **Intelligence-Related Communications Infrastructure.** The joint intelligence communications subarchitecture encompasses collection, processing, exploitation, analysis, and dissemination nodes. These nodes are supported by a robust communications infrastructure and automated systems equipped with tailored applications to meet the broad array of intelligence activities. **Command, Service, and combat support agency intelligence processes rely on a communications backbone consisting of JWICS and SIPRNET.** This infrastructure is supplemented by a distributed, common exploitation and dissemination system, tactical data links, and intelligence broadcast services.

(1) **Joint Worldwide Intelligence Communications System.** JWICS is the IC's global communications network that provides DOD and IC users a mature, reliable, and flexible SCI communications architecture. JWICS is designed to deliver secure, assured, efficient, interoperable information on a global basis to national and defense intelligence consumers.

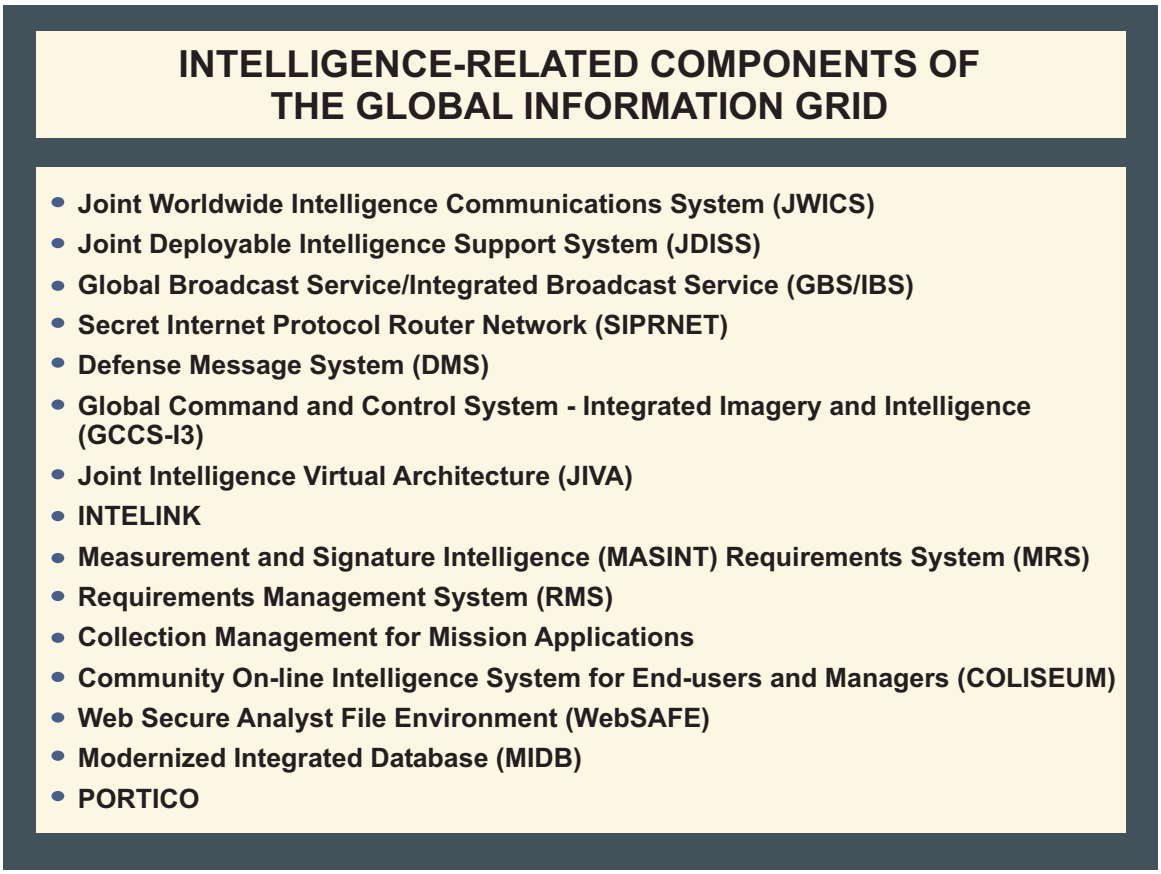


Figure V-1. Intelligence-Related Components of the Global Information Grid

JWICS provides real-time SCI data and video teleconferencing and connects deployed forces, on land and at sea, with their parent commands, the Services, national intelligence producers, senior DOD leadership, and other federal agencies.

(a) JWICS is best described as a multiplexer-based secure (Top Secret/SCI), high-speed multimedia intelligence communications network. JWICS meets the requirements for dedicated, interactive, and high bandwidth video-capable communications. The strategic objective of JWICS is to provide interoperable and responsive intelligence communications connectivity for the military IC. This effort has included the development of JWICS in three modes (i.e., fixed, containerized, and mobile) with the capability of supporting a joint force or NIST in a fixed structure and/or field site.

(b) The complementary architecture of JWICS (data and/or video) and JDISS workstations (data) spans strategic, operational, and tactical levels. The major JWICS applications are: electronic publishing; video teleconferencing; and bulk data transfer including very large file imagery.

(c) Containerized JWICS (C-JWICS). C-JWICS is a lightweight, deployable JWICS capability developed to support contingency requirements through the use of military or commercial satellites or terrestrial earth terminals. C-JWICS II is the current iteration. The C-JWICS II supports SCI video, data, and National Secure Telephone System (NSTS).

(d) JWICS Mobile Integrated Communication System. JMICS provides a scaleable, deployable JWICS that is self-contained on a heavy, high mobility, multipurpose, wheeled vehicle (HMMWV) for rapid deployment in all weather, austere environments. Key features include satellite connectivity, FAX, Nonsecure Internet Protocol Router Network (NIPRNET), SIPRNET LAN, SCI LAN workstations, JDISS network servers, and SCI video teleconferencing equipment. JMICS is controlled by Joint Staff J-2O and is deployed in support of NIST or joint force requirements.

(2) **Joint Deployable Intelligence Support System.** JDISS bundles commercial off-the-shelf hardware and software applications in a standard desktop environment. JDISS provides a field-deployable office automation suite built upon the system security infrastructure provided by client-server environment system services. JDISS also allows electronic mail and chat between intelligence echelons via the site's existing communications architecture. JDISS provides access to theater, Service, and national intelligence resources, such as databases, basic imagery analysis and dissemination capabilities, specific analytical tools, and support functions required to execute the intelligence mission.

(3) **GBS** is an information service that is based on commercially developed direct broadcast technology to provide a wide range of information, including intelligence and intelligence products, to the warfighter. This simplex broadcast system uses both military and leased commercial satellite capacity to provide high bandwidth capacity for broadcast of information such as imagery, video, environmental data, logistics, and warning to all command levels.

(4) **SIPRNET** is the Secret-level wide-area network (WAN), with a worldwide backbone router system. Various DOD router services and systems are migrating onto the SIPRNET backbone router network to serve the long-haul transport needs of the users. This network supports national defense C4I requirements.

(5) **DMS** is an application layer messaging system that relies on the NIPRNET, SIPRNET, and JWICS for message transport. DMS is used to exchange messages electronically between DOD organizations in a fixed location or tactical environment, and ensures messaging interoperability with allies, coalition partners, non-DOD USG agencies, and other US and foreign organizations.

b. **Intelligence-Related Information Processing, Storage, and Management Systems.** The "Communications Handbook for Intelligence Planners (U)" provides more information on the systems briefly described below. These components of the GIG consist of information processing, storage, and management applications specifically tailored to meet the broad array of intelligence activities supporting joint military operations.

(1) **GCCS-I3** provides the commander and staffs with ready access to imagery and intelligence through a standard set of integrated, linked tools and services. It enhances the commander's battlespace awareness and maximizes commonality and interoperability across tactical, theater, and national-levels.

GCCS-I3 operates in both joint and Service-specific environments and is deployed in both SCI and collateral domains.

(2) **JIVA** is a set of information processing and management applications that permit intelligence personnel to enroll in and attend on-line training courses, facilitate collaborative intelligence analysis and production among geographically disparate analysts, and enable the rapid analysis of multi-source streams of data.

(3) **INTELINK** is a principal electronic means for intelligence product dissemination. INTELINK builds on ongoing architectural initiatives at the Top Secret/SCI and Secret and Unclassified classification levels (see Figure V-2). INTELINK provides a comprehensive set of tools to query, access, and retrieve information. INTELINK permits collaboration among policy developers, analysts, and users, and will simplify access to a wide variety of services. The J-2 should assess the availability of INTELINK access among assigned and en route forces. The J-2 should also ensure that users have adequate system training and are aware of available products, content, and access procedures.

(4) **MRS** provides national and DOD intelligence organizations with a common MASINT requirements submission and tracking system.

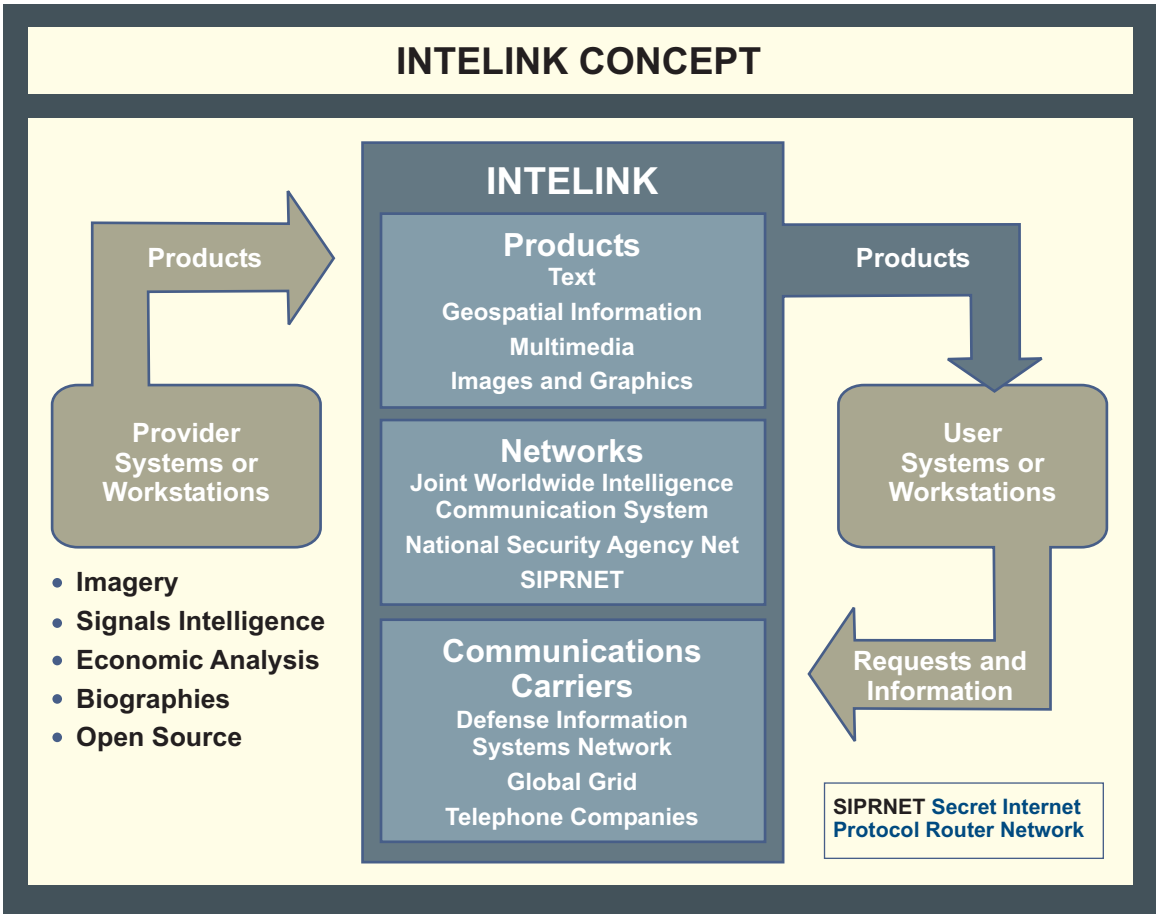


Figure V-2. INTELINK Concept

(5) **Requirements Management System** provides the national and DOD imagery communities with a uniform automated collection management system.

(6) **Collection Management for Mission Application (CMMA).** CMMA is accessed through GCCS and comprises a tailorable suite of interoperable automated tools designed to enhance the collection planning, execution, and ISR battle management capability of combatant commands, subordinate joint forces, and components. CMMA includes PRISM (planning tool for resourcing, integrating, synchronizing, and management), which is used in collection planning, operations, and managing of intelligence collection assets that are deployed to all combatant commands and USFK.

(7) **COLISEUM** is a database application that allows the user to identify and track the status of all validated intelligence production requirements and RFIs.

(8) **Web Secure Analyst File Environment** provides intelligence analysts with the means of retrieving classified message traffic, intelligence information reports, and abstracts of hardcopy all-source intelligence documents produced by DIA.

(9) **MIDB** provides sets of data elements and the capability to relate items of intelligence information with other items within the database itself; for example, relating OB information to installations.

(10) **PORTICO** is a web-based system designed to improve the quality, availability, timeliness, and sharing of information across the DOD CI community to facilitate common situational awareness.

c. **Other Communication Resources**

(1) **The Joint Communications Support Element (JCSE).** The USJFCOM JCSE is a unique communications organization that provides contingency and crisis communications to meet the operational and support needs of the JCS, Services, combatant commands, Defense agencies and non-Defense agencies. Requests for support should be completed IAW CJCSI 6110.01A, *CJCS-Controlled Communications Assets*. The JCSE provides tactical communications support for two simultaneously deployed subordinate joint forces and two joint special operations task forces. The JCSE possesses a wide range of communications capabilities tailored to meet a variety of contingency missions, including intelligence.

(2) Army, Marine Corps, and Special Operations Forces use TROJAN SPIRIT II, JMICS, and tactical LAN in support of joint requirements for intelligence support to subordinate joint forces and NIST. These systems provide communications connectivity to support full JWICS, JDISS data, secure voice, and other unique intelligence communication needs.

(3) Liaison with other agencies or Service elements with communications capabilities, such as NSA or a public affairs group, may reveal existing or available communications links in place. While

these organizations have their own requirements, in a crisis the J-2, in coordination with the J-6, may arrange to temporarily share their circuits to meet critical needs.

3. Combatant Commander's Communications Planning

A wide range of national, theater, and component intelligence and communication systems are available to a JFC. The existence of this capability does not, however, ensure that intelligence and communications systems can be deployed without significant planning and coordination. Supporting communications paths will probably have to be procured or extended to link the JFC with the GIG. **The theater J-2 must understand current systems sufficiently to tailor an architecture integrating intelligence sensors, processors, dissemination systems, databases, information systems and communications systems. The J-2 needs to maximize the use of the in-theater communication resources and then deploy ancillary equipment to extend the communications links to the warfighter.** Since the preferred equipment or communications paths may not be available for a quick reaction to a contingency, alternative systems and/or subsystems and communications paths may have to be used or procured. The subordinate joint force J-2 must effectively coordinate communications architecture requirements with the J-6 and coordinate with the J-4 and other logistic elements for the timely delivery and installation of intelligence and communications systems. In addition, communications systems requirements for national-level connectivity for NIST support should be forwarded to the Joint Staff J-2 for validation and tasking. The combatant command or the joint force J-6 should coordinate with the NIST for communications planning and support. Interoperability problems need to be addressed and resolved during the planning phase.

a. **Communications Planning Methodology.** Key concepts to successful intelligence systems support are joint interoperability, streamlined flow of information, and providing pull-down of intelligence tailored to the needs of the operating forces. The ability to provide the tactical commander with real/NRT intelligence continues to be a critical factor. The following steps provide a useful methodology for planning an intelligence communications architecture (see Figure V-3):

(1) In planning a communications architecture, step 1 includes identifying the type of mission, the CONOPS, joint and Service doctrine, and the specific mission requirements. Step 1 functions are developed to meet specific mission objectives of the JFC and each of the subordinate commanders and an operational scenario for the mission. Step 1 products include lists of the subordinate joint force composition and the assets assigned from national, theater, and Service levels, and a specific activity timeline for operations planned by the JFC and each subordinate commander.

(2) In step 2 the specific communication intelligence support plan for the joint force is determined by the mission and the intelligence support concept developed by the component commanders in the operational area. This model identifies the intelligence functions required to support the subordinate JFC and the intelligence information flows required to support each function.

Figure V-3. Joint Force Intelligence Communications Planning Methodology

(3) Step 3 compiles the intelligence information flows from step 2 into a node-to-node layout of intelligence information transactions. Nodes are used to represent the HQ and the external supported and/or supporting organizations. This is done by numbering the nodes of interest and developing needlines. A needline represents the flow from one node to another.

(4) During step 4 the joint force J-6 staff will determine the communications support plan for requirements identified in step 3. The requirements developed by the J-2 planning staff can either be analyzed separately or combined with similar inputs from the J-1, J-3, J-4, J-5 and J-6 staffs at each security level.

b. **Architecture Planning**

(1) In the past, planning for external subordinate joint force exchanges was accomplished by multiple organizations, resulting in redundant communications. Interoperability was hindered by a lack of governing architecture, resulting in dissemination requirements not being satisfied. Combatant commanders planned their connectivity to the subordinate joint force, and the national intelligence agencies planned their connectivity to the NIST at the subordinate joint force. These requirements should be planned collectively rather than independently, thus ensuring an integrated communications support plan is developed.

(2) The combatant command J-2 and J-6 should plan and set up adequate communications paths for the JFC and/or subordinate joint force intelligence needs prior to operational deployment (see Figure V-4). The joint force should use established WANs as the basis for planning its communications, information systems support, and dissemination to the joint force component commanders at the Top Secret/SCI and Secret levels. In coordination with the J-6, the J-2 builds a tailored, integrated architecture that incorporates sensors, processors, and dissemination systems with information systems and

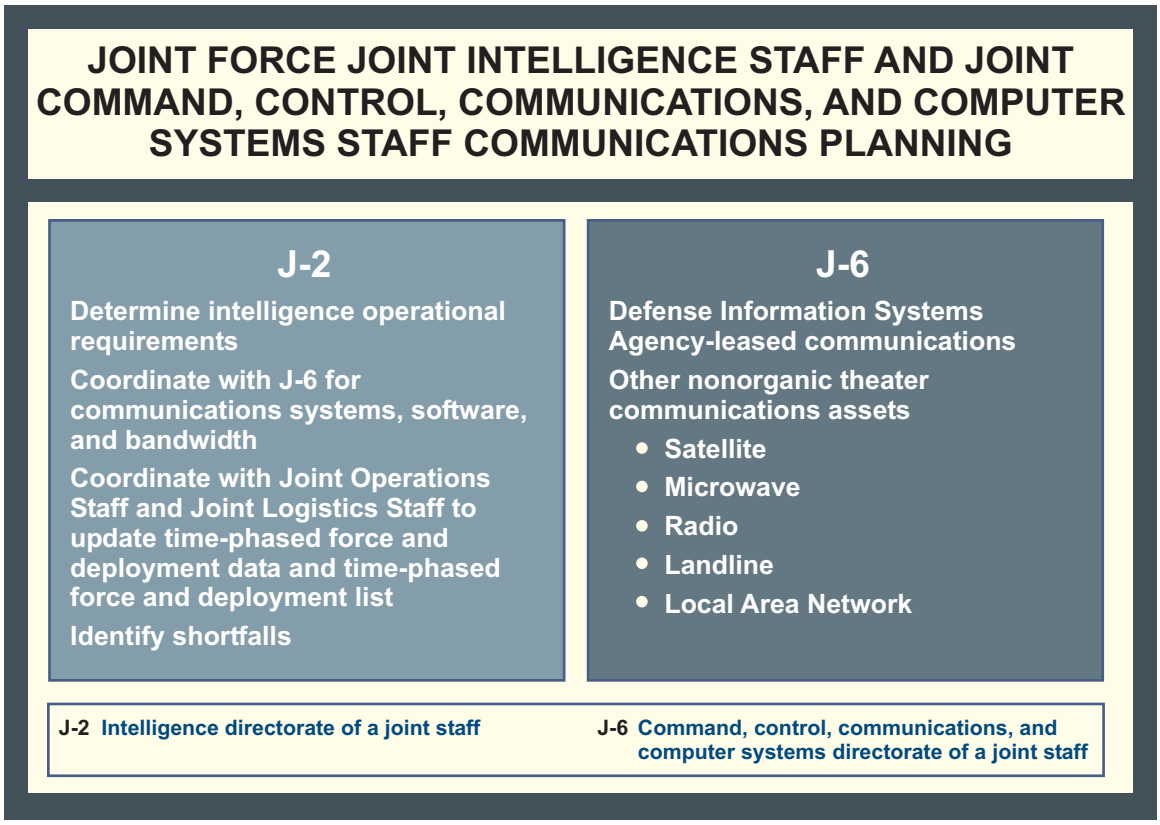


Figure V-4. Joint Force Joint Intelligence Staff and Joint Command, Control, Communications, and Computer Systems Staff Communications Planning

communications systems (e.g., JWICS). This architecture links the subordinate joint force with the Service components and coalition or allied units as well as with the combatant commands and the NMJIC. The major components of the joint intelligence architecture provide connectivity between the joint force and the national and component levels. This tailored architecture includes prototype equipment and units with different or unique systems. Once the architecture is defined, the J-2 works with the J-3 and J-4 to update the TPFDD. The J-2 and J-6 should solve any interoperability problems prior to resource deployment.

c. **System Planning**

(1) Organic communications asset requirements must be identified to the J-6. As soon as the subordinate joint force J-2 determines operational and dissemination requirements, the J-2 coordinates support from the subordinate joint force J-6 for the necessary communications systems, communications security (COMSEC), application software, and communications bandwidth needed to provide simultaneous transmission of secure, interactive video teleconferencing; dissemination of selected products using graphics, desktop publishing, data, and secondary imagery; and secure voice. Shortfalls in communications support are identified and submitted to higher HQ for resolution.

(2) Subordinate joint force communications links include satellite, microwave, radio, landline, and LANs. The subordinate joint force J-2 and J-6 identify the proper frequencies, communications

protocols, network security management requirements, encryption devices, and procedures for the architecture components. The resulting communications capability interfaces with the global intelligence infrastructure, i.e., the national IC, the combatant command JIC, the subordinate joint force and components, and allies and/or coalition partners.

(3) Requests to the combatant command J-6 for DISA-leased or nonorganic theater communications resources may become complex. For example, if requesting a WAN service such as JWICS, the subordinate joint force will likely need Joint Staff and DISA coordination and DIA and/or NSA requirement validation. The J-6 requires detailed information for formal request documentation. Information required includes the type of telecommunications support required, proposed location, time required to be operational, duration, funding and justification. For a circuit requirement, the request should indicate terminal types at all locations; estimated intelligence traffic volumes; precedence and security levels; types of available encryption; specific locations; POC; any recommended restoration priority; usage duration; and type of circuit special considerations. The subordinate joint force prepares a telecommunications request for service and submits it to the appropriate command or J-6 validating authority. This process can be completed in advance by establishing contingency or oncall circuitry activation IAW an approved OPLAN.

(4) The standard tactical entry point and teleport sites make this process easier, using existing Defense Satellite Communication System strategic earth terminals and commercial earth terminals to provide warfighters with a standardized set of pre-positioned circuits for entry into the GIG. These sites serve as a C4I communications hub to maximize satellite resource efficiency and access to services.

d. **Planning Considerations**

(1) Joint intelligence dissemination relies on "pull/push" concepts. The "pull" concept allows JFCs to acquire relevant intelligence when needed, based on their mission and the specific phase of the ongoing operation, using intelligence databases physically located and maintained at various locations. Additionally, the theater JIC should determine the location of the desired intelligence and "push" the necessary information directly to all echelons requiring it.

(2) Every subordinate joint force operation requires planning for the exchange of intelligence within a deployed joint force and between the deployed joint force and supporting intelligence organizations. Intra-subordinate joint force communications should support the exchange of situation data, RFIs, intelligence, and tasking of organic collection resources among the major elements of the deployed joint force and supporting intelligence organizations worldwide. These exchanges include the following:

(a) Intelligence exchanges within and between each component assigned or attached to the subordinate joint force. Each Service and functional component should deploy with an organic tactical communications capability that meets intra-Service exchange requirements.

(b) Exchanges between the HQ of the subordinate joint force and, if designated, the HQ of the components. Any intra-subordinate joint force requirements for intelligence exchanges at lower echelons can either be routed through these HQ or identified as special requirements that must be planned separately.

(c) Connectivity requirements of the subordinate JFC to the combatant commander and to the national intelligence support agencies (e.g., connectivity for the NIST that may deploy to support the subordinate JFC), to other supporting commanders and, in special cases, to other subordinate joint forces.

(d) Connectivity requirements from the assigned components to Service intelligence centers in theater and CONUS must also be addressed.

(e) Exchanges between the HQ of the joint force and supporting crisis intelligence federation partners operating from home stations.

(f) Connectivity with and among coalition intelligence partners.

(3) The requirement to exchange large quantities of perishable data among dispersed forces places special demands on many communications networks. Additionally, commanders and planners must understand the possible adverse effect large volumes of intelligence data may have on a limited bandwidth transmission system. Combatant commanders will determine the priorities of C4 systems and allocate communications circuits and channels (bandwidth) within the geographic AOR of their commands, including those required by component and other subordinate commands.

THE PEARL HARBOR WARNING MESSAGE

Even the best of intelligence is useless if it fails to arrive in time to support the decision maker. Just hours prior to the Japanese attack on Pearl Harbor, US code breakers reading Japanese diplomatic traffic convinced Army Chief of Staff Marshall to send a message to US forces in the Pacific alerting them to the possibility of a Japanese attack at approximately 0800 hours on 7 December. The following account of how Marshall's warning message was tragically mishandled that fateful day is condensed from Rear Admiral Layton's book "And I Was There."

"Colonel Bratton [Chief of the Army G-2 Far Eastern Section] arrived at the Munitions Building shortly before nine. He was reading the fourteenth part of the Tokyo message and comparing it with the previous afternoon's thirteen parts when he was handed a much shorter message that had just been decrypted: 'Will the ambassador please submit to the United States Government (if possible the Secretary of State) our reply to the United States at 1:00 p.m. on 7th, your time.'

'This immediately stunned me into frenzied activity because of its implications,' Bratton testified. 'The vital factor in my mind was the date and hour of delivery of the 14-part message.' That Tokyo would want a diplomatic message delivered on a Sunday was unusual enough, but the specific timing was its real significance. Dawn was an ideal time to launch a surprise attack, and a brief look at a time chart left Bratton 'convinced the Japanese were going to attack some American installation in the Pacific area.'

Nearly two hours had elapsed from the receipt of the deadline message to the time that General Marshall arrived at his office. Marshall eventually agreed that another alert should be 'sent at once by the fastest possible means.' Despite the 'awful urgency' about beating the deadline, which was little more than an hour away, for security reasons Marshall did not want to use the scrambler telephone.

Time was running out, as Bratton well appreciated. When he arrived at the signal center he was 'very much exercised,' according to Colonel Edward F. French who was in charge of the army's signal center. Bratton had to translate Marshall's hastily scrawled dispatch, which read:

'Japanese are presenting at one p.m. eastern standard time today what amounts to an ultimatum. Also they are under orders to destroy their code machine immediately. Just what significance the hour set may have we do not know but be on the alert accordingly. Inform naval authorities of this communication. Marshall.'

Marshall might have changed his mind about using the Navy facilities, or his scrambler telephone, to reach General Short [Commander, US Army Hawaiian Department] if French had reported that heavy static had blocked out the Army's radio circuits to Honolulu since 1030. When French learned of this holdup, he decided to send the message to Hawaii using his teleprinter link to the Western Union Washington office.

Because the coded telegram containing Marshall's warning had been inadvertently sent out without a priority designation, when it reached the RCA Honolulu office at three minutes after the deadline had expired in Washington, it was pigeonholed for routine delivery to Fort Shafter.

Kimmel [Commander in Chief, US Pacific Fleet] stood by the window of his office at the submarine base, his jaw set in stony anguish. As he watched the disaster across the harbor unfold with terrible fury, a spent .50-caliber machine gun bullet crashed through the glass. It brushed the admiral before it clanged to the floor. It cut his white jacket and raised a welt on his chest. 'It would have been merciful had it killed me,' Kimmel murmured to his communications officer, Commander Maurice 'Germany' Curts.

Tadeo Fuchimaki, the RCA messenger who had been delayed for more than an hour and a half in the panicky traffic jams, finally gunned his motorbike up to the gates of Fort Shafter. The communications staff was flooded with incoming and outgoing reports, so it was almost four hours before anyone thought of decoding the low-priority cable from Washington. When Short finally saw a copy of Marshall's warning, it was nearly eight hours old.

Military annals have provided few more glaring examples of information that arrived too late to change the course of history. To his dying day Admiral Kimmel considered the delayed warning of Tokyo's one o'clock deadline as the most shocking example of Washington's mishandling of the whole matter of intelligence."

SOURCE: Rear Admiral Edwin Layton, USN (Retired),
***"And I Was There," Pearl Harbor and Midway – Breaking the Secrets*,**
William Morrow and Company, Inc., New York, 1985

(4) Required communications capabilities considered by J-6 and J-2 planners includes channel capacity, defined as the maximum rate at which information can be sent over a communication channel without error. Imagery transmission requirements are of particular concern because of their high bandwidth requirements, which are directly proportional to the degree of resolution desired (i.e., the higher the resolution, the longer the transmission time via a given bandwidth). The J-6 and J-2 planners must ensure that high bandwidth transmissions such as imagery do not preclude or delay the receipt of other transmissions (e.g., messages), affecting the operation. Wideband circuits required to resolve this problem are costly and not always available in intratheater locations. While satellite transmission systems offer high volume and broad coverage (compared to landline and line of sight [LOS] radio systems), overall transmission capacity is limited to the radio frequency spectrum and how the combatant commander apportions available satellite bandwidth. Landline system capacity is limited by the amount of wire or fiber in place throughout the system.

4. Multinational Force Intelligence and Communications Interoperability

a. Multinational operations are becoming the norm for military operations, making intelligence-sharing with allies and coalition partners increasingly important. **A multilevel security system does not currently exist that can easily facilitate sanitization and dissemination of intelligence to US and allied and/or coalition operational commanders.** However, combatant commands and subordinate joint forces can request that intelligence products be made releasable to coalition and/or allied nations as necessary.

b. A subordinate joint force should be interoperable with, and have access to, theater-information systems and databases, as well as allied and/or coalition force and component command systems such as LOCE and STONEGHOST. LOCE is the primary automated system for exchanging intelligence with NATO allies, while the STONEGHOST system is used to disseminate intelligence among the US, United Kingdom, Canada, Australia, and New Zealand. A similar interoperability exists in Korea with

the Pacific Information Systems Server Site-Korea. However, CENTRIXS defines the standards for establishing and maintaining multinational connectivity at the tactical and operational level, with reachback capability to the strategic level. The basic CENTRIXS operational architecture framework is the same for all combatant commands and leverages existing networks, technology and network centers. CENTRIXS services include email, web, chat, and COP capabilities and uses controlled interfaces for two-way information flows among US military commands and multinational partners.

APPENDIX A
JOINT FORCE J-2 QUICK REACTION CHECKLIST

1. Overview

This checklist can assist a subordinate joint force J-2 and staff by providing a quick reference guide during a crisis situation. This is a guideline or point of departure, and should not be construed as all-inclusive. Depending upon the nature of the crisis (war or military operations other than war [MOOTW]), many of these variables may or may not apply. Other considerations not listed may also become factors.

2. Establish Missions and/or Tasks

a. Clarify and prioritize the subordinate joint force J-2's missions, tasks, and requirements with input from the subordinate joint force J-3.

b. Determine WMD reconnaissance assets and coverage areas for organic, remote, and stand-off WMD MASINT resources.

c. Assist the J-3 in development of mission objectives and determining the potential availability of the intelligence/information required to support the JFC's decisions, guidance, and intent relative to the joint mission.

d. Ensure distribution and complete understanding of the tasking and guidance from the commander, and that it has been analyzed and applied to regional and/or theater assessments. Update or revise assessments, if necessary, to conform to the commander's guidance.

e. Ensure that regularly updated intelligence collection and production priorities are passed throughout the entire chain of command, including components and supported commands.

f. Determine theater architecture for intelligence responsibilities. Intelligence responsibilities must be clearly delineated among subordinate joint force, combatant command, and national levels. Determine whether any subordinate joint force units (SOF in particular) require intelligence support from the combatant command or national level that the theater JIC cannot provide.

g. Determine theater intelligence architecture for flow of secure communications, collection, dissemination, and information systems assets. Identify problems regarding coordination, interoperability of systems, or supply issues.

h. Determine status (number, type, readiness condition) of subordinate joint force's organic intelligence collection, production, exploitation, dissemination and communications assets.

i. Verify that all intelligence personnel and equipment are listed in the appropriate priority on the TPFDL.

j. Conduct liaison, supervise, and coordinate other intelligence-related functions with appropriate staff elements and subordinate and supporting commands. Specific responsibilities include the following:

(1) IO (J-3). IO core capabilities include:

(a) Electronic warfare (EW) (J-3, or EW officer when assigned).

(b) Military deception (J-3).

(c) Psychological operations (PSYOP) to include an estimate of target audience conditions and vulnerabilities, susceptibility, and accessibility of prospective target groups; an estimate analysis of the effectiveness of friendly PSYOP and adversary propaganda; and planning assistance for the joint psychological operations task force or joint special operations task force (whichever is applicable) and supervision of training activities concerning defense against adversary propaganda (J-3).

(d) Operations security (J-3).

(e) Computer network operations (J-3).

(2) Counterproliferation (J-3).

(3) Counterintelligence (J-2).

(4) ISR (J-2 and J-3).

(5) Counterterrorism (J-3).

(6) Antiterrorism and/or force protection (J-3).

(7) Handling of enemy prisoners of war (EPWs), enemy combatants (ECs), detainees, and captured documents and materiel (J-1/J-3/J-4).

(8) Debriefing of EPW and refugees, exploitation of captured documents and equipment (J-2/J-3/J-4).

(9) Transportation intelligence (USTRANSCOM/J-2).

(10) Adversary employment of special weapons (WMD) (J-3 and/or WMD officer).

(11) CA, to include BDA, munitions effectiveness assessment, and future targeting or reattack recommendations (J-2 and J-3).

(12) Medical intelligence (staff surgeon and/or DIA).

(13) Civil-military operations (J-3).

(14) Barrier and denial operations (J-3).

(15) Personnel recovery (including survival, evasion, resistance, and escape) (J-3).

(16) Language capabilities of subordinate joint force personnel (J-1).

(17) Classified courier issues (J-1).

(18) Geospatial information and services (GI&S officer).

(19) Blue force situational awareness and combat identification requirements (J-3).

3. Identify Support Needed

a. **Intelligence Services and/or Products**

(1) Identify available intelligence assets in-theater, including information systems and/or tools.

(2) Determine whether there is a requirement for Service, theater, or national intelligence agency support (e.g., NIST, USJFCOM, QRT, JWICS, DOCEX). If so, identify entities to be tasked and mix of skills and capabilities needed. Identify proper chain of command for requests.

(3) Identify and analyze crisis intelligence federation requirements. Request activation or modification of existing crisis intelligence federations or the formation of new federation partnerships in support of the JFC.

b. **Personnel.** Ensure that required and/or additional expertise is available, with sufficient personnel to meet watchstanding, courier, security and liaison requirements.

(1) Identify any requirements for personnel augmentation, to include regional or functional experts, linguists, and/or reservists.

(2) Determine augmentation support that can be obtained from theater assets. Coordinate tasking for those assets through the combatant commander's staff.

(3) Determine augmentation support that must be obtained from outside the theater. Coordinate with the J-1 as early as possible in the planning process to request support from external sources.

(4) Assume that the operation for which the subordinate joint force was established will continue for an extended period of time, then make plans to request and accommodate rotation of staff and support elements and additional augmentation.

(5) Identify any need for a deployable element to support the subordinate joint force's efforts in collection management, CI/HUMINT collection, Service expertise, communications, tactical or in-depth analysis, debriefing, DOCEX, and polygraph support.

(6) Identify any needed requirements for a deployable MASINT element to support the subordinate joint force's efforts.

c. **Logistics**

(1) In concert with the combatant command J-2 and the subordinate joint force J-2, J-3, and J-4, ensure that transportation requirements for high priority personnel and materiel are documented and prioritized. If this is an unforeseen contingency or crisis, there will not be existing TPFDD for personnel and materiel, and the J-2 must assist the J-4 to ensure that intelligence needs are documented and met.

(2) Ensure that transportation requirements for high priority intelligence personnel and or materiel are in concert with J-3 requirements.

d. **GI&S Support.** Shortfalls of critical GI&S products and digital data severely restrict the planning and analysis phases and may hinder operations during the execution phase. Early coordination with NGA and other GI&S producers is essential. Outdated or missing geospatial data may negatively impact the ability of forces to accomplish the mission.

(1) Initiate single GI&S POC. Notify subordinate forces of correct requisition procedures for predeployment maps, charts, and digital data.

(2) Notify combatant command GI&S staff of the GI&S support POC in the subordinate joint force.

(3) Identify subordinate joint staff GI&S requirements to the combatant command GI&S staff with respect to forces deploying and the operational area. Include map production quantities, personnel and equipment to operate a map depot, and staff support personnel.

(4) Request the following from the combatant command GI&S staff: the production schedule; status of products and digital data required and date of first shipment; status of host-nation support (HNS) for GI&S products, digital data and capabilities; and the status on disclosure and/or release of geospatial information to coalition forces.

(5) Verify and/or submit OPORD Annex M to J-2.

(6) Request that supporting forces provide a GI&S distribution plan. Ensure that combatant command and joint force GI&S staffs are provided a copy of all distribution plans.

(7) Send a message reminding forces about accuracies, datums, and coordinates of GI&S products and digital data.

(8) Coordinate shipment of deployment stock to the map depot. Obtain weight, cubic feet, number of pallets and ready-for-shipment date from the combatant command GI&S staff. Forward unit line number to the combatant command GI&S staff.

(9) Establish map depot inventory quantities to include reorder levels. Report results to the combatant command GI&S staff via DMS message, electronic mail, or JDISS.

(10) Request that the combatant command GI&S staff have NGA publish a special operation catalog.

e. **METOC Support.** METOC support can help optimize intelligence support in a variety of ways (assisting in collection management, helping to anticipate adversary actions). Coordinate with the joint force METOC officer through the J-3, if applicable, for needed METOC products and services and for the transfer of METOC data received through intelligence resources that could supplement the METOC database.

f. **MASINT Support.** MASINT support will help optimize intelligence support by enhancing the product and providing a more comprehensive view of the COP.

g. **DOCEX Support.** DOCEX support will assist deployed maneuver elements and/or the ground component command in initially establishing a document exploitation capability in a remote or distant area of operations.

4. Establish a JISE

a. Determine whether a JISE is required to support the subordinate joint force. Establishment of a JISE will be theater and/or situation dependent.

b. If a JISE is to be established, consider the following:

(1) Facility location and physical security requirements.

(2) Personnel requirements, including augmentation.

(3) JISE structure requirements for:

(a) Collection Management Section.

(b) Intelligence Support Section.

(c) Targeting Support and BDA Section.

(d) Other intelligence production.

(e) Communications and information systems support.

(f) Soft-copy and/or electronic and hard-copy product dissemination to components;

(g) Receipt, processing and exploitation of imagery and production of imagery-based materials.

(h) Establishment of subordinate joint force JISE relationships and connectivity to component, combatant command, and national intelligence.

(i) Supplies needed for a lengthy deployment, if a JISE or other intelligence element is forward-deployed.

(j) Force protection and physical security.

(k) Military deception.

(l) Counterintelligence support.

c. Develop intelligence communications architecture with reporting and requesting channels.

5. Intelligence Collection Management

a. In concert with the combatant command J-2 and the subordinate joint force J-3, ensure that all intelligence collection requirements are identified as early as possible.

b. Develop and publish intelligence collection requirements. Establish time schedule for updates.

c. Identify organic collection capabilities and status of all component and supporting units as well as those en route to the operational area.

d. Identify any shortfalls in collection capabilities relative to the joint force's validated intelligence requirements. Ensure that collection requirements to cover such shortfalls are developed and forwarded through the combatant command JIC to the DIA Office of Collection Management for subsequent national resource tasking.

e. Prepare an ISR CONOPS that fully integrates the capabilities of all organic, coalition, allied and commercial ISR assets and resources and that maximizes the efficiency of the tasking, processing, exploitation and dissemination architecture. Forward ISR CONOPS to Joint Staff J-2/J-3 with all requests for forces and with all OPLANs.

f. Ensure that collection activities are coordinated with the Defense Collection Coordination Center through the combatant command JIC and the DIA Office of Collection Management for subsequent national resource tasking.

g. HUMINT collection

(1) Establish the need for a subordinate J-2X to manage, coordinate and deconflict HUMINT, CI, country team and/or SOF collection activities. Coordinate with the combatant command J-2, HSE and CISO for requesting required resources from the DHS and the Services and appointment of HOC and TFCICA.

(2) Establish the need for a joint interrogation and debriefing center (JIDC) and joint document exploitation center (JDEC) (see Appendix G, "Joint Exploitation Centers") to satisfy subordinate joint force and combatant command PIRs. Request staffing from the components and the DHS, as required.

(3) Establish the need for and request further HUMINT collection augmentation and support from the DHS.

h. IMINT collection

(1) Obtain emergency dissemination authority for imagery and imagery products. Emergency dissemination authority is a powerful tool, designed to support military operations, including those involving allies.

(2) Tailored imagery should be requested as soon as a target is identified. All imagery should be forwarded to requester.

(3) Establish the need for and request further IMINT collection augmentation and support from the Services or national imagery agencies.

i. SIGINT collection

(1) Coordination of SIGINT support for JTF operations should be accomplished through the command's organic cryptologic support division in concert with the respective CSG and command NCR.

(2) Establish the need for and request further SIGINT collection augmentation and support from the Services or NSA.

j. MASINT collection

(1) Coordination of MASINT support for JTF operations should be accomplished through the command's MASLO.

(2) Establish the need for and request further MASINT collection augmentation and support from the Services and the DIA MASINT/Technical Collection Directorate.

k. All other intelligence disciplines.

6. Intelligence Production Management

a. Coordinate with theater JIC to determine whether PIRs have already been established for current situation. PIRs are built around commander's operational requirements.

b. As needed, in concert with J-3 and theater JIC, tailor PIRs for current situation.

c. Keep PIRs current and update periodically.

d. Develop or acquire a complete intelligence assessment of the situation.

(1) Periodically update situation assessment.

(2) Submit completed situation assessment to the commander and chain of command.

e. Ensure regional and threat assessments are current.

f. Ensure key friendly and neutral forces have been identified.

g. Coordinate the theater and national assessments and provide copies to subordinates and components.

h. Ensure all required intelligence annexes have been incorporated into the OPLAN or OPORD.

i. Closely track intelligence collection and production requirements to completion.

7. C4 Support (For Subordinate Joint Force Intelligence)

a. The J-2 should establish and maintain regular dialogue with the combatant command J-2 and the Service component intelligence staff officers.

b. Request JCSE support/augmentation.

c. As soon as possible, coordinate with the J-6 to ensure communications lines are available.

d. Know the capacity of communications paths serving the subordinate joint force, between the subordinate joint force and its components and with allied or coalition units.

(1) Assess the C4 capabilities and requirements of all assigned intelligence elements and those en route to the operational area.

(2) Intelligence exchange with allied and/or coalition units may require a liaison with secure portable communications and information systems support.

(3) Minimize. Keep communications paths open by eliminating extraneous traffic. Units with global missions routinely subscribe to numerous summaries from all theaters. Assign lowest possible precedence on summary messages. Cancel summaries for the subordinate joint force staff and components and rely on tailored support from the JIC.

e. Fully apprise subordinate joint force and senior commanders of all relevant current events.

f. Ensure subordinate joint force J-2s' information systems equipment is compatible with theater and subordinate systems. For coalition forces, ensure systems are compatible.

g. Ensure communications lines have sufficient rate capacity or bandwidth.

h. If necessary, establish a tactical SCIF.

i. Identify COMSEC needs (devices, keying material) and determine availability.

j. Ensure all router tables are updated.

k. Ensure all DMS addresses are updated, complete and used.

l. Eliminate duplicate data being disseminated to the same users by different means.

m. Ensure information systems security measures are employed properly.

n. Determine reporting/production times and types of reports.

8. Multinational Interaction

a. Establish liaison between joint and multinational force intelligence organizations.

b. Ensure procedures have been established and reviewed to expedite sanitization and sharing of US-generated intelligence products with allies and coalition partners.

c. Ensure friendly objectives, intentions, and plans are fully communicated to appropriate intelligence organizations.

d. Ensure interoperability of C4 systems.

e. Be aware of, and remain sensitive to, cultural and/or religious differences among allies and coalition members. In some instances, these may result in periods of increased vulnerability for the joint force, or may require scheduling changes for meetings and/or briefings.

9. Counterintelligence

a. In coordination with the J-3 and multinational intelligence and/or CI elements, develop and implement CI and counterterrorism plans.

b. The CISO should recommend to the J-2, appointment of either a TFCICA, or counterintelligence operational tasking authority upon the establishment of a JTF.

c. Ensure CI functions/activities are incorporated into planning, especially force protection planning.

d. Ensure CI is included in collection management planning.

e. Advise component CI organizations and begin planning coordination with the Joint CI Division and other combatant command CISOs for national-level joint CI assistance.

f. Ensure intelligence security guidelines have been developed and disseminated.

g. Ensure the development and required approval of a CI Force Protection Source Operations umbrella concept.

h. Ensure early deployment of CI assets in order to provide critical threat/vulnerability assessments as necessary.

Additional information on CI can be found in JP 2-01.2, Joint Doctrine, Tactics, Techniques, and Procedures for Counterintelligence Support to Operations.

10. Security

a. Ensure personnel and information security measures, including those applying to information systems, are enforced throughout the joint force.

b. Enforce need-to-know criteria for release of all information related to the operation.

APPENDIX B
NATIONAL INTELLIGENCE

Editor's Note: This appendix incorporates the material currently resident in JP 2-02, *National Intelligence Support to Joint Operations*, which will be eliminated upon the approval of JP 2-01.

Annex A Joint Centers
B Other Governmental Organizations
C Intelligence Systems in Support of Crisis Operations
D Intelligence Resource Programs

NATIONAL INTELLIGENCE

"Tell me what you know . . . tell me what you don't know . . . tell me what you think . . . always distinguish which is which."

General Colin Powell
Chairman of the Joint Chiefs of Staff, 1989-1993

1. Introduction

The joint force J-2 will have to rely on national intelligence organizations for support in order to provide the JFC with timely, relevant, and accurate intelligence. The J-2 must understand how the national intelligence organizations are organized and how they operate in order to best exploit their capabilities. This appendix provides information about the national-level intelligence organizations that could provide support to joint operations.

2. Management and Oversight of the Intelligence Community

a. **National Security Act.** The National Security Act of 1947 created the framework for the IC. The act established the NSC, DCI, and DOD, and identifies the organizations that make up the IC.

b. **National Security Council.** The NSC is the principal forum to consider national security issues that require Presidential decision (see Figure B-1). There are four statutory members: the President, the Vice President, the Secretary of Defense, and the Secretary of State. The Chairman of the Joint Chiefs of Staff and the DCI serve as statutory advisors. The DCI attends NSC meetings as its intelligence advisor. The Assistant to the President for National Security Affairs (the National Security Advisor) is responsible for the NSC's day-to-day operations. Council functions are supported by the NSC staff that includes the White House Situation Room and regional and functional desks.

c. **Director of Central Intelligence.** As the top policymaker for the IC, the DCI develops policies for and provides guidance on future intelligence needs and capabilities. The DCI is authorized to establish committees and boards for advice, and is charged with producing and disseminating national foreign intelligence. The DCI tasks major collection systems that can be employed to satisfy strategic, operational, and tactical intelligence requirements. The DCI also is responsible for coordinating the relationships between elements of the IC and the intelligence or security services of foreign governments on all matters involving intelligence related to the national security or involving intelligence acquired through clandestine means; providing overall direction for the collection of national intelligence through human sources by elements of the IC and coordinating with other agencies that are authorized to undertake collections; and conducting CI activities outside the US and coordinating the CI activities of other government agencies outside the US. The DCI serves in four roles:

(1) As the principal intelligence advisor to the President.

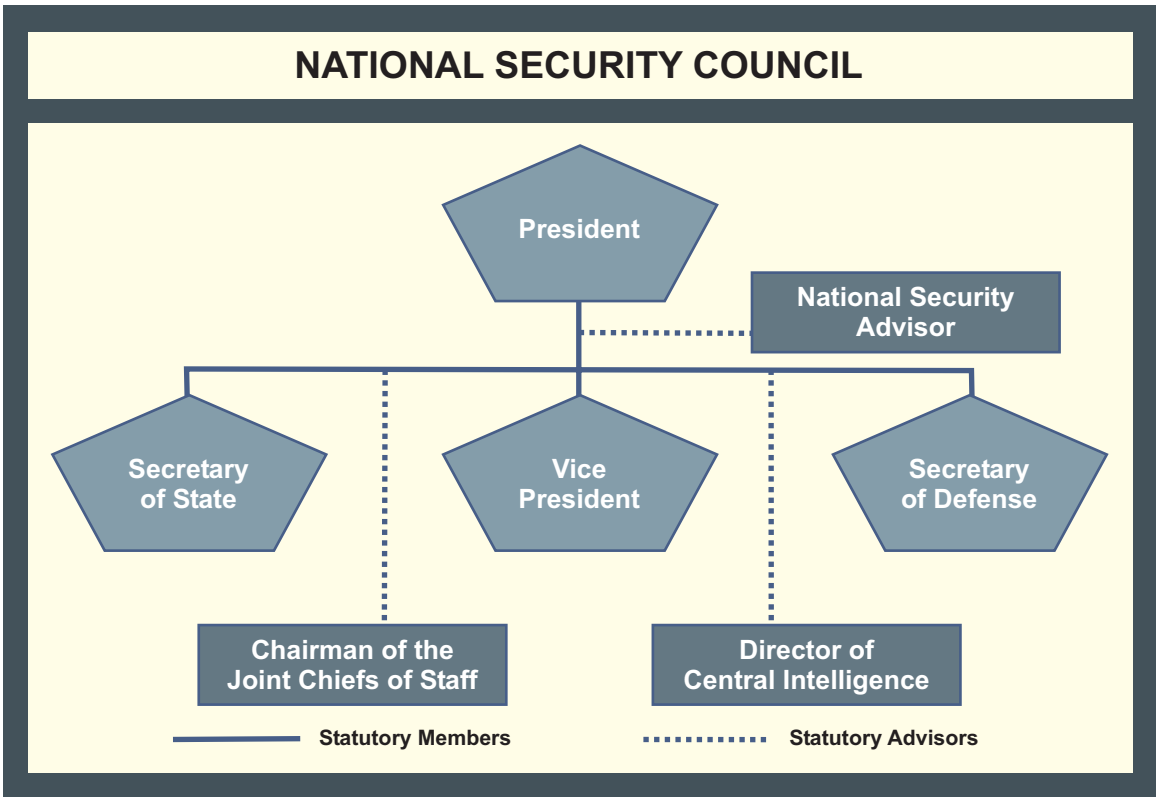


Figure B-1. National Security Council

(2) As the director of the CIA.

(3) As the head of the entire US IC.

(4) As a statutory advisor to the NSC.

d. **Intelligence Community.** The IC is a federation of executive branch agencies and organizations that work separately and together to conduct intelligence activities necessary for the conduct of foreign relations and the protection of US national security. (The IC currently includes CIA; NSA; DIA; NGA; NRO; State Department; Department of Homeland Security; the CI, cryptologic, and some of the foreign intelligence elements of the Military Services (Army, Navy, Air Force, and Marine Corps); and foreign intelligence and/or CI elements of the FBI, USCG, and the Treasury and Energy Departments.

(1) **IC Management.** Two key officials directly support the DCI in implementing the DCI's community responsibilities.

(a) **Chairman, National Intelligence Council (NIC).** The Chairman of the NIC **oversees IC production and analysis,** including national intelligence estimates and NIC memorandums.

(b) **Deputy Director of Central Intelligence for Community Management (DDCI/CM).** The DDCI/CM develops, coordinates, and implements DCI policies and exercises the DCI's

responsibilities in planning, programming, and budget development; requirements management and evaluation; strategic planning; collection management; analysis and production; and acquisition oversight. The DDCI/CM supervises the Executive Director for Intelligence Community Affairs, who is responsible for directing the Community Management Staff (CMS).

(2) **Community Management Staff.** The CMS is responsible for oversight of IC responsiveness to the DCI's guidance. The CMS oversees all IC-wide programming and budgeting activities and controls the overall requirements tasking process. The principal CMS offices, and the contribution each makes in promoting the overall effectiveness of the IC, are as follows:

(a) **Resource Management Office** is responsible for NFIP budget development, evaluation, justification, and monitoring.

(b) **Program Assessment and Evaluation Office** is responsible for creating a process that allows the DCI to shape the NFIP, and helps evaluate intelligence programs based on their support to US national security missions.

(c) **Requirements, Plans and Policy Office (RPPO)** supports the DCI's development and promulgation of policy to guide IC activities. RPPO evaluates the IC's performance in responding to current national intelligence requirements; develops organizational and procedural architectures for DCI initiatives; addresses IO, security policy, IC-related aerospace policy, and human resource issues; and coordinates IC foreign language issues.

(3) **National Foreign Intelligence Advisory Groups**

(a) **The President's Foreign Intelligence Advisory Board (PFIAB).** The PFIAB consists of 16 members, appointed by the President, who are senior civilian and former military leaders. The Board reports directly to and advises the President on the performance of all government agencies engaged in the collection, analysis, or production of intelligence or in the execution of intelligence policy. Additionally, the Board advises the President concerning the objective, conduct, and coordination of the activities in these agencies. The Board is specifically charged to make appropriate recommendations for actions to improve and enhance the performance of intelligence efforts.

(b) **The National Foreign Intelligence Board (NFIB).** The NFIB is the senior IC advisory body to the DCI and includes senior representatives from all organizations involved in the collection, processing, and analysis of intelligence. The intelligence chiefs of the military Services are observers. The Board is chaired by the DCI and reviews all substantive intelligence matters, including production, review, and coordination of all national foreign intelligence; arrangements with foreign governments on intelligence matters; and protection of intelligence sources and methods.

(c) **Intelligence Senior Steering Group (ISSG).** The ISSG is chaired jointly by the DDCI/CM, the Under Secretary of Defense (Intelligence) (USD(I)), and the Joint Staff

Directorate for Force Structure, Resource, and Assessment (J-8), and is comprised of senior representatives from IC organizations. It provides oversight of major intelligence systems requirements, development, acquisition, architecture and related intelligence issues.

(d) **Intelligence Community Principals Committee (ICPC)** and **Intelligence Community Deputies Committee (ICDC).** These committees consider and develop policies, plans, and processes for DCI decisions on key issues of concern to the IC. The ICPC is chaired by the DCI or Deputy DCI and includes the directors of the major IC agencies. The ICDC is chaired by the DDCI/CM and includes the deputy directors of the major IC agencies. It resolves important policies, plans, and processes not requiring the attention of the ICPC or the DCI.

3. Nonmilitary Members of the Intelligence Community

The efforts of non-DOD members will primarily focus on strategic intelligence and support to the President and Secretary of Defense (see Figure B-2). These agencies identify global and regional issues and threats to the President and Secretary of Defense, military leadership, and combatant commanders. This responsibility includes assessing potential issues and situations that could impact US national security interests and objectives. Intelligence provided by these agencies is essential in support of some military operations, particularly MOOTW. The following descriptions of the non-DOD members of the IC include subordinate offices which support IC activities but are not necessarily considered a part of, or funded by, the IC.

a. **Central Intelligence Agency**

Figure B-2. Nonmilitary Members of the Intelligence Community

(1) CIA's primary areas of expertise are in HUMINT collection, imagery, all-source analysis, and the production of political and economic intelligence. The CIA has three Deputy Directors: Deputy Director for Operations; Deputy Director for Intelligence; and Deputy Director for Science and Technology. The DCI is also the head of the CIA, but there is an Executive Director who handles the day-to-day activities of the agency.

(2) **Office of Military Affairs (OMA).** The OMA falls under the Associate Director of Central Intelligence for Military Support, a flag rank military officer. OMA is staffed by CIA and military personnel. As the agency's single POC for military support, **OMA negotiates, coordinates, manages, and monitors all aspects of agency support for military operations.** This support is a continuous process that can be enhanced or modified to respond to a crisis or developing operation. Interaction between OMA and the DCI representatives to the OSD, the Joint Staff, and the combatant commands facilitates the provision of national-level intelligence in support of joint operations, operation planning, and exercises.

(3) **Foreign Broadcast Information Service (FBIS)**

(a) The FBIS is the primary collector of foreign open-source information for the IC. The FBIS collects comprehensive foreign open-source information on developing world events and trends for the President, Cabinet, senior US policymakers, and government agencies.

(b) FBIS brings the latest foreign political, military, economic, and technical information to the intelligence analysis, warning, and operations processes. FBIS monitors approximately 2,350 publications, 331 radio stations, 153 television stations, 112 news agencies, 70 Internet sources, and 40 databases in 210 countries and 73 languages.

(c) FBIS administers CONUS and outside the continental United States (OCONUS) installations in support of its mission to collect, translate, analyze, and disseminate information responsive to US policy interests from the world's open-source media, including radio, television, press agencies, newspapers, periodicals, journals, books, maps, databases, gray literature, and the Internet.

(d) The FBIS accepts formal open-source collection tasking from the IC through the HUMINT process. IC customers that want to levy standing open-source collection need to identify their requirements to the National HUMINT Requirements Tasking Center during the formulation or revision of collection directives. Additionally, FBIS accepts formal tasking from the CIA's Directorate of Intelligence Production through the Directorate's Collection Requirements and Evaluation Staff.

(e) On a case-by-case basis, FBIS will consider ad-hoc collection tasking requests from IC organizations and agencies (including CIA), depending on available resources. Requests for ad-hoc collection efforts by FBIS should be addressed to the FBIS Information Center for proper referral.

(f) FBIS makes available to the IC and other USG agencies the following products and services derived from foreign open-sources:

1. **FBIS Reporting.** FBIS, through its worldwide access to foreign media and other publicly available materials, provides political, military, economic, and technical information. Translations of the information are collectively referred to as FBIS "reporting." FBIS databases of reporting are accessible either from several worldwide electronic information handling systems that function via the Internet or similar technology, or from one of FBIS' own proprietary mechanisms such as CD-ROM.

2. **FBIS Observations and Analysis.** FBIS analyzes the content and behavior of the media of countries posing a significant policy interest to the USG's foreign affairs community.

3. **FBIS Video Products.** FBIS provides television program summaries and selected video programs to a limited set of customers.

4. **Foreign Language Glossaries.** FBIS officers skilled in foreign languages produce on an ad-hoc basis glossaries or guides to foreign language terminology, which the National Technical Information Service hosts on its Fed World service on the Internet (http://www.fedworld.gov/fbis).

5. **World Wide Guides.** FBIS foreign media experts compile catalogs of information about the electronic and print media of a specific country or region, providing broadcast and circulation figures as well as political affiliations and policy positions.

6. **Maps.** FBIS supports USG agencies by providing unclassified reference maps and geographic information.

7. **Publications Procurement.** FBIS procures foreign media and other forms of open-source information, including newspapers, journals, books, newsletters, commercial annual reports, telephone directories, CD-ROMs, and databases for USG components participating in the Foreign Publications Procurement Program.

8. **Gray Literature Procurement.** FBIS obtains gray literature (publicly available material that cannot be obtained by commercial subscription) in response to specific customer requests and standing collection directives. FBIS maintains the Gray Literature Tracking Database, which is available on the INTELINK-TS and Open-Source Information System network.

9. **FBIS Operations Center.** The FBIS Operations Center is a 24-hour watch office that serves as a major conduit between FBIS HQ, FBIS OCONUS installations, and numerous USG operations centers.

10. **Linguistic Support.** On a fee-for-service basis, FBIS selectively provides a variety of linguistic services to its USG customers, including reverse translations, emergency translations, foreign language instruction, translations from audio and videos, classified translations, and assistance to treaty monitoring efforts.

b. **Department of State**

(1) **Bureau of Intelligence and Research.** The INR coordinates programs for intelligence, analysis, and research and produces intelligence studies and current intelligence analyses essential to foreign policy determination and execution.

(2) **Bureau of Politico-Military Affairs.** The Bureau originates and develops policy guidance and provides general direction on issues that affect US security policies, military assistance, nuclear policy, nonproliferation policy, and arms control matters. This office maintains political and military liaison with the DOD and other Federal agencies on a wide range of affairs.

(3) **Bureau of International Narcotics Matters.** The Bureau develops, coordinates, and implements international narcotics control assistance activities. It is the principal point of contact and provides policy advice on international narcotics control matters for the Office of Management and Budget, the NSC, and the White House Office of National Drug Control Policy (ONDCP). The Bureau also oversees and coordinates the international narcotics control policies, programs, and activities of US agencies.

(4) **Foreign Service.** Ambassadors are the personal representatives of the President and report to him through the Secretary of State. The President gives the chief of the diplomatic mission, normally an Ambassador, direction and control over all US in-country government personnel except those assigned to an international agency or to a combatant commander.

c. **Department of Energy.** The Office of Nonproliferation and National Security directs the development of the Department's policy, plans, and procedures relating to arms control, nonproliferation, export controls, and safeguard activities. Additionally, this office is responsible for managing the Department's research and development program for verifying and monitoring arms implementation and compliance activities, and for providing threat assessments and support to HQ and field offices.

d. **Federal Bureau of Investigation.** The FBI, the principal investigative arm of the Department of Justice, **has primary responsibility for CI and counterterrorism operations conducted in the United States**. CI operations contemplated by any other organizations in the United States must be coordinated with the FBI. Any overseas CI operation conducted by the FBI must be coordinated with the CIA.

e. **Department of the Treasury.** Intelligence-related missions include the production and dissemination of foreign intelligence relating to US economic policy and participation with the DOS in the overt collection of general foreign economic information.

f. **United States Coast Guard, Department of Homeland Security.** The USCG has unique missions and responsibilities as both an armed force and a law enforcement agency that make it a significant player in several national security issues. To accomplish these diverse objectives the USCG

intelligence program consists of two distinct elements — the National Intelligence Element and the Law Enforcement Intelligence Program. The National Intelligence Element conducts activities as described in Executive Order 12333 and the National Security Act of 1947, and is a part of the IC. USCG intelligence efforts support counterdrug operations, alien migration interdiction operations, living marine resource enforcement, maritime intercept operations, port status and/or safety, counterterrorism, coastal and harbor defense operations, and marine safety and/or environmental protection.

(1) The USCG Intelligence Coordination Center (ICC) is a tenant command within the US Navy's NMIC in Suitland, Maryland, and maintains a 24-hour intelligence watch, providing I&W input to the NMIC. The ICC acts as the strategic center with ties to both national intelligence agencies and the HQ-level law enforcement intelligence activities. The ICC supports strategic analysis, manages Coast Guard collection, and provides national imagery exploitation support, including tactical support to operational commanders.

(2) USCG Area Intelligence components provide regional and operational intelligence for USCG operations through the Atlantic and Pacific Maritime Intelligence Fusion Centers. Coast Guard intelligence entities have the capability to access SIPRNET, Navy and IC databases and C4I systems, including JWICS, the Anti-Drug Network, and the Joint Maritime Information Element.

(3) USCG Investigative Service (CGIS) is a federal investigative and protective agency chartered to conduct internal and external criminal and personnel security investigations, assist in providing personal security protection, and conduct counterintelligence investigations. Responsibilities include: criminal investigations of maritime crimes, investigating fraud, personal protection services, and security background investigations. CGIS CI and intelligence operations focus on drug smuggling, environmental crimes, illegal immigration by sea, and assistance as required by other federal law enforcement agencies.

(4) USCG National Response Center (NRC) serves as the central national point of contact for reporting environmental intelligence data for all oil, chemical, radiological, biological and etiological discharges into the environment in the United States and its territories. The NRC gathers and distributes intelligence data for federal on-scene coordinators and serves as the communication and operations center for the deployable National Response Team.

g. **Department of Homeland Security.** The Department of Homeland Security's Directorate for Information Analysis and Infrastructure Protection (IAIP) provides I&W support to the Homeland Security Advisory System, assesses the scope of terrorist threats to the US homeland, and integrates terrorist-related information from other Department of Homeland Security components, other USG agencies, State and local government authorities, and private sector entities. IAIP provides intelligence analysts to the DCI Terrorist Threat Integration Center, which prepares and provides comprehensive terrorist threat-related assessments to the President and USG agencies. The Department of Homeland Security also conducts intelligence collection activities under the auspices of the US Customs Service. US Customs Service intelligence activities include an aerial surveillance arm and intelligence analysis centers. While the primary purpose of Customs intelligence activities is to stem the illegal smuggling of aliens and merchandise

with intent to avoid paying duties, information collected and produced by the Customs Service can contribute directly to homeland security and counterterrorism.

4. Military Intelligence Community

a. **Responsibilities of the Office of the Secretary of Defense.** As shown in Figure B-3, the Secretary of Defense, assisted by the USD(I), exercises full authority, direction, and control over the intelligence activities of DOD. The Secretary of Defense is responsible for collecting, processing, producing, and disseminating military and military-related foreign intelligence and counterintelligence. As a member of the NSC, the Secretary of Defense participates in the development of national-level policy. The Secretary of Defense has a major responsibility to ensure timely development and submission of proposed national programs and budgets.

(1) **Defense Intelligence Executive Board (DIEB).** The DIEB is the senior corporate advisory body to the Secretary of Defense for review and oversight of defense intelligence programs and activities. Further, the DIEB is the senior management body providing fiscal and programmatic guidance to the Joint Military Intelligence Program (JMIP). Upon the establishment of the JMIP, the Secretary of Defense created the DIEB as a management mechanism to " . . . provide effective oversight of Defense Intelligence programs and to make key decisions for efficient allocation of available resources to address Department needs." The DIEB is chaired by the Deputy Secretary of Defense, with the USD(I) serving as its executive secretary. Additional members include the DCI; representatives of the Military Services; a number of senior OSD officials; the Vice Chairman of the Joint Chiefs of Staff; the Director of the Joint Staff; and the directors of all Defense agencies involved in the JMIP.

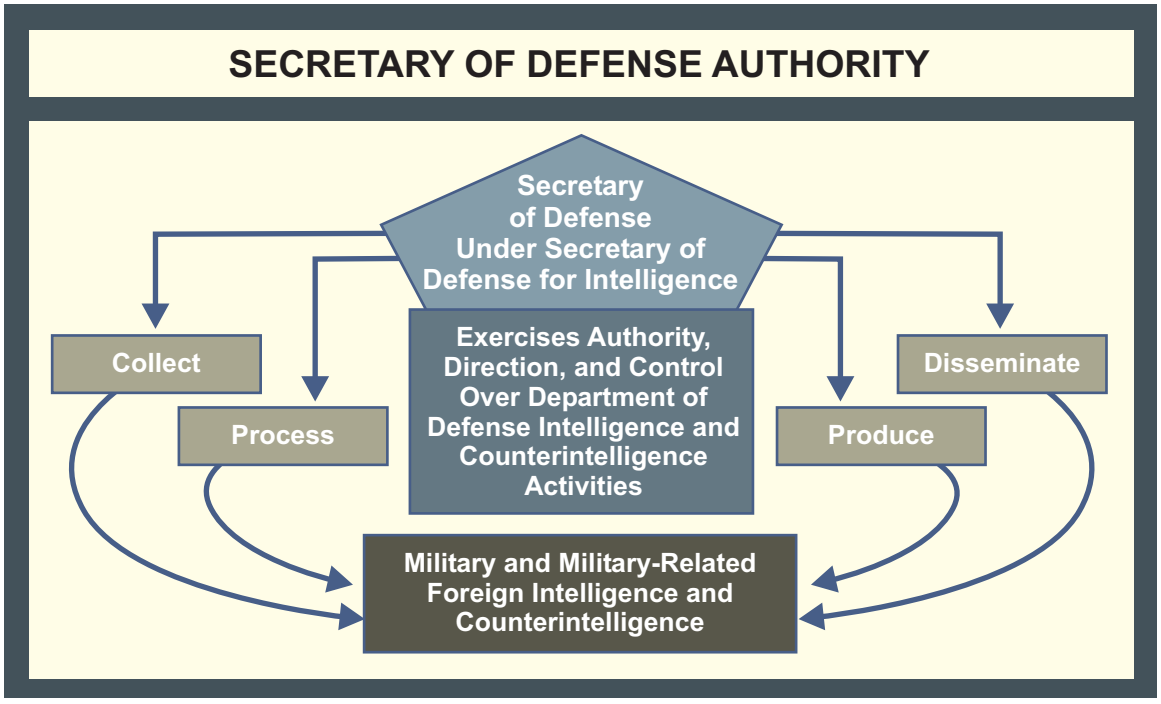


Figure B-3. Secretary of Defense Authority

(a) **DIEB Issues.** The DIEB provides a forum for discussion and review of existing and emerging issues and challenges for intelligence in support of defense needs and develops immediate solutions when necessary. The composition of this board ensures significant issues are identified and addressed. Through careful corporate examination of defense intelligence capabilities, **the DIEB develops alternatives and recommendations that foster the most effective allocation of these resources.** The board meets not less than twice a year to provide advice and counsel on defense intelligence issues.

(b) Discussions and advisory guidance focus on requirements, policy, interoperability, resources, priorities, and goals.

(2) **USD(I).** The USD(I) is the principal staff assistant and advisor to the Secretary of Defense on all intelligence, counterintelligence and security, and other intelligence-related matters. On behalf of the Secretary of Defense, the USD(I) exercises authority, direction, and control of intelligence and counterintelligence organizations within DOD to ensure that they are manned, trained, equipped and organized to support DOD missions and are responsive to DCI requirements. The USD(I) also exercises authority, direction, and control over CIFA (for further information regarding CIFA refer to Annex B, "Other Governmental Organizations," of this appendix). The USD(I) is assisted by the following deputies:

(a) **The Deputy Under Secretary of Defense (Preparation and Warning)** is responsible for long-range (10-15 years) forecasts and assessments regarding the nature of the future security environment. These assessments are designed to help prepare DOD for discernible changes in areas such as science and technology, deployment of new types of weapons systems and changes in regional relationships and balances. This long-range security outlook will permit DOD leaders to adjust acquisition strategies and programs, force deployments, and coalition and alliance planning and structuring.

(b) **The Deputy Under Secretary of Defense (Intelligence and Warfighting Support)** provides assistance to the Services and combatant commands in identifying their intelligence support requirements and helps ensure those requirements are met with organic DOD assets or other IC resources.

(c) **Deputy Under Secretary of Defense (Counterintelligence and Security)** provides guidance to, and overseeing the activities of, the DOD counterintelligence community. This includes defending the security of DOD personnel, facilities, processes, information, and computer network systems.

(d) **Deputy Under Secretary of Defense (Policy Requirements and Resources)** is responsible for planning, programming and budgeting activities pertaining to the JMIP and tactical intelligence and related activities (TIARA) budgets. This includes coordinating with other USD(I) elements to formulate programmatic recommendations, and working with the combat support agencies to ensure their budgets satisfy DOD intelligence requirements.

(3) **Assistant to the Secretary of Defense (Intelligence Oversight).** The Assistant to the Secretary of Defense (Intelligence Oversight) conducts independent oversight inspections of DOD intelligence and CI activities, including DOD use of law enforcement information, to ensure compliance with legal requirements and standards of propriety. This office also reviews all allegations that raise questions of legality or propriety involving intelligence or CI activities in the Department of Defense, to ensure that investigations are properly accomplished and appropriate corrective measures are implemented.

b. **The Military Intelligence Board (MIB).** The MIB serves as the senior "Board of Governors" for the Military IC and works to develop cooperation and consensus on cross-agency, Service, and command issues. The MIB is chaired by the Director of DIA. The membership of the MIB is shown in Figure B-4.

(1) The MIB is a key element involved in guiding and supporting DOD intelligence operations. **The MIB coordinates intelligence support to military operations** and provides a forum for the discussion of issues going before the NFIP, CMS, and other national-level intelligence forums.

(2) The MIB may assist in obtaining intelligence support to military operations during periods of crisis or contingency operations within a combatant command's AOR. During major combat operations the MIB meets on an almost daily basis to address theater intelligence shortfalls identified by combatant commanders and to coordinate the deployment of needed personnel, equipment, and systems to support operations.

5. Defense Intelligence Agency

DIA is a combat support agency and a major intelligence planner, collector and producer in the Defense IC. DIA is responsible for managing military and military-related intelligence and counterintelligence requirements of the Secretary of Defense and Deputy Secretary of Defense, Chairman of the Joint Chiefs of Staff, other DOD components, and non-DOD agencies of the federal government when appropriate. Its mission is to provide timely, objective, and cogent military intelligence to commanders — and to DOD and USG decision makers and policymakers. DIA's support to policymakers focuses on developing national-level intelligence assessments, presenting and providing perspectives for defense policy, and providing I&W of potential crisis.

a. **Responsibilities.** The Director, DIA advises the Secretary of Defense and Deputy Secretary of Defense, the Chairman of the Joint Chiefs of Staff, combatant commanders, and USD(I) on all matters concerning military and military-related intelligence; is the principal DOD intelligence representative in the national foreign intelligence process; and, with the agreement of the heads of DOD intelligence components, is responsible for coordinating the budgeting and allocation of DOD intelligence component personnel and resources to satisfy DOD intelligence requirements. DIA's support flows across a wide spectrum of military activities to include: counterintelligence, counterterrorism, counterdrugs, medical intelligence, counterproliferation mission support to combat WMD, United Nations peacekeeping and coalition support, personnel recovery

Figure B-4. Membership of the Military Intelligence Board

and prisoner of war/missing in action, missile and space intelligence, noncombatant evacuation efforts, targeting, and BDA. DIA responsibilities include the following:

(1) Providing peacetime, crisis, contingency, and combat intelligence support to the operational military forces.

(2) Providing military intelligence support for the policy and planning activities of DOD components and, as appropriate, for similar activities of non-DOD national authorities.

(3) Planning, programming, and budgeting activities in support of DOD intelligence missions to include the following (see Annex D of this Appendix, "Intelligence Resource Programs," for greater detail on the individual programs):

(a) Serving as the Program Manager of the General Defense Intelligence Program (GDIP); developing the GDIP as an input to the NFIP; participating in the NFIP approval process; and overseeing execution of funds appropriate for GDIP and GDIP-related activities.

(b) Preparing and submitting the DIA program and budget input to the GDIP, the DOD Foreign Counterintelligence Program, and the JMIP.

(c) Serving as the program coordinator of the Defense General Intelligence and Applications Program (DGIAP) of the JMIP.

(d) Assembling and developing statements of military intelligence requirements and related plans, programs, and budget proposals, and advising the Chairman of the Joint Chiefs of Staff, USD(I), DCI and other DOD components, as appropriate.

(e) Responding to requests by the USD(I) and Chairman of the Joint Chiefs of Staff to review and provide recommendations concerning planning, programming, budgeting, and the use of intelligence resources for the collection and production of intelligence in support of planning and operations requirements of military forces in peacetime, crisis, contingency, and combat situations.

(4) Providing representation on national and international fora.

(5) Conducting intelligence activities for which DIA is assigned responsibility, the implementation of which require personnel and resources from one or more of the other DOD intelligence components, and exercising the degree of direction and control over these personnel resources that is required to accomplish the purpose of the activities.

(6) Fostering joint cooperation in the activities of DOD intelligence components and enhancing coordination among these components.

(7) Fostering interoperability of all DOD intelligence systems at all levels.

(8) Providing support to the Chairman of the Joint Chiefs of Staff for, and participating in, the implementation of sensitive support programs.

(9) Coordinating and, when appropriate, developing and executing the intelligence annex to OPLANs.

b. **Organization.** DIA is organized into seven directorates and the Joint Military Intelligence College, in addition to the staff comprising the Command Element (see Figure B-5). These Directorates are discussed below.

(1) **The Joint Staff Directorate for Intelligence, J-2.** The Joint Staff J-2 is a unique organization, in that it is both a major component of DIA, as well as a fully integrated element of the Joint Staff. Joint Staff J-2 is composed of several deputy directorates, three of which make up the core of the NMJIC: Crisis Management (J-2M), Crisis Operations (J-2O), and Targets (J-2T). The organization, missions and functions of the NMJIC have already been discussed in detail in Chapter II, "Joint and National Intelligence Organizations, Responsibilities, and

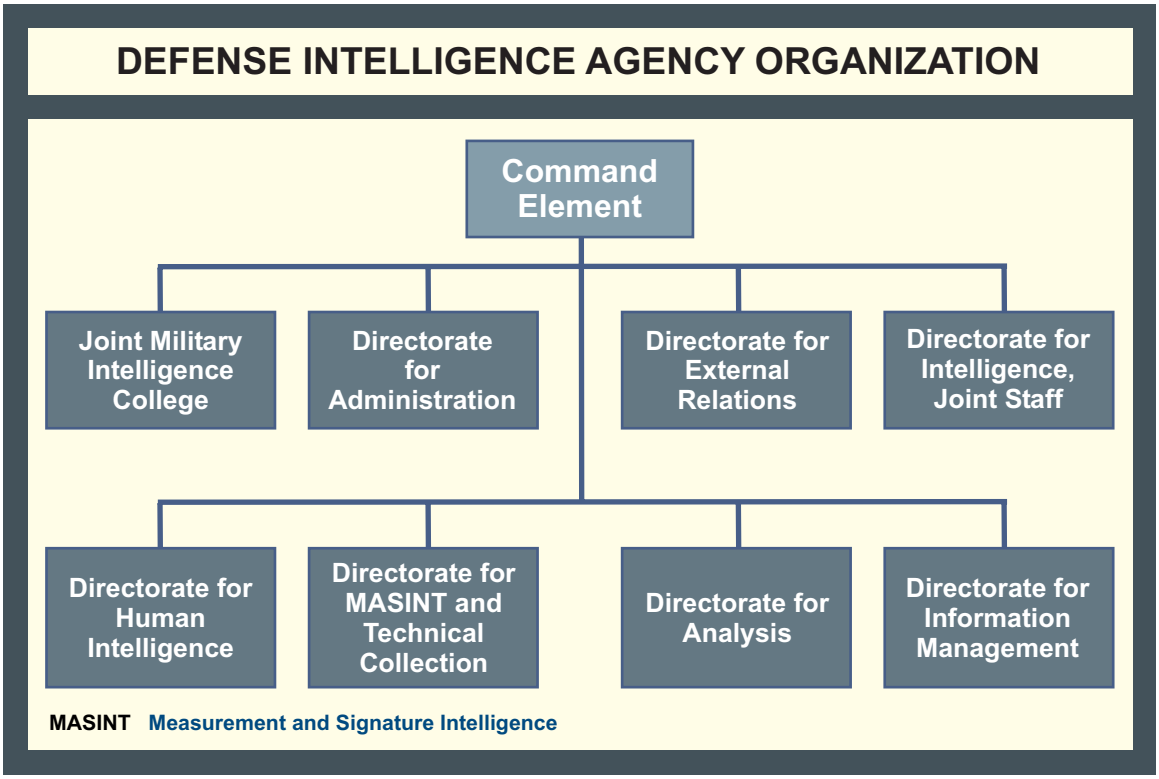


Figure B-5. Defense Intelligence Agency Organization

Procedures," Section B, "National Intelligence." The other deputy directorates are Administration (J-2A), Joint Staff Support (J-2J), and Assessment, Doctrine, Requirements, and Capabilities (J-2P) and are described below.

(a) **Deputy Directorate for Administration.** J-2A focuses on all personnel, budget, manpower, and infrastructure issues for the Joint Staff J-2. All J-2 personnel and security issues are centralized in this directorate to support J-2 and the IC representatives resident in the NMJIC. It is the central clearinghouse for all information systems requirements necessary to support the J-2 and its operations.

(b) **Deputy Directorate for Joint Staff Support.** J-2J serves as the DIA focal point for supporting the Chairman of the Joint Chiefs of Staff, maintains close relationships with all offices of the Joint Staff, and ensures prompt and responsive DIA participation and support in intelligence matters. J-2J also serves as the Joint Staff J-2 Military Secretariat, and receives, tasks, monitors, and ensures suspense dates are met on all Joint Staff actions.

(c) **Deputy Directorate for Intelligence Assessments, Doctrine, Requirements, and Capabilities.** J-2P assesses intelligence-related joint warfighting capabilities for the CJCS Joint Requirements Oversight Council (JROC) to assist JCS prioritization of high-payoff capabilities. J-2P also develops joint intelligence doctrine, architectures, strategies, and policies that directly support combatant commands and subordinate JFCs worldwide. Specific responsibilities include the following:

1. Leading and conducting the battlespace awareness joint warfighting capabilities assessments for the JROC; acting as the secretariat for the functional concept board (intelligence); and providing management and guidance and developing consensus among the IC, combatant commands, Services, Defense agencies and organizations, and OSD.

2. Integrating existing studies, data, and analyses for assessments of baseline ISR capabilities and programs; developing a future vision of ISR support to joint warfighting; identifying gaps in capabilities and shortfalls in ISR systems and programs; and recommending improvements and new initiatives for consideration by the JROC and OSD in their development of the key CJCS and SecDef planning and programming guidance.

3. Developing capabilities to perform comprehensive analyses of ISR requirements, capabilities, and resulting architectures; developing and maintaining an interactive, multimedia and data access system; and providing all-source intelligence information, sensor characteristics, C4I data, organizational relationships, equipment quantities and locations, and associated programmatic information to support assessments of ISR architectures.

4. Ensuring that joint intelligence doctrine and intelligence support to information operations are structured to support forces operating throughout the range of military operations.

5. Developing and maintaining joint, multinational, and combined intelligence doctrine and TTP.

6. Conducting liaison with the IC, including representing and monitoring the Defense IC and combatant commands or Service requirements for intelligence and intelligence-related capabilities and systems.

7. Ensuring that joint intelligence requirements are incorporated in both DCI and DOD planning, programming, and prioritization documents.

8. Serving as the Intelligence Requirements Certification Office for the IC.

9. Coordinating and facilitating military intelligence issues between the military intelligence and C2 communities.

10. Representing the Joint Staff J-2 in the programmatic and budgetary review of proposed and/or operational community and Defense intelligence programs.

11. Participating in the development of DCI, OSD, and CJCS program guidance documents.

(2) **Directorate for Analysis.** DI produces the broadest range of intelligence for support to joint operations of any organization in the IC. As the Functional Manager for Production, DI also manages the production of military intelligence throughout the Defense IC in response to

the needs of DOD and non-DOD customers. DI's defense intelligence officers, with regional and functional responsibilities, provide the bridge among policymakers, intelligence collectors, and the J-2. In anticipation of crisis, and during crisis or deployed US military operations, DI draws on analytic expertise throughout the Defense IC and, where appropriate, from non-Defense agencies. DI directs analytical elements in Washington, DC and the production efforts of two field production activities: AFMIC and MSIC. The OICC, located in the DIAC, serves as the crisis management office for the DI in direct support of DIA and/or the J-2 and is the single point of contact in DI for requirements involving analytical support. Other DI responsibilities include the following:

(a) Participating in and supporting, as appropriate, the activities of the Defense Special Missile and Astronautics Center, IC centers, committees, and working groups established by the DCI, and comparable activities established by the Secretary of Defense.

(b) Preparing intelligence assessments and estimates concerning transfers of technology, goods, services, and munitions (including associated transfer mechanisms) and participating in interagency, national, and international fora on such transfers.

(c) Establishing product standards for, exercising technical and quality control over, overseeing the establishment of requirements for, and managing the nonduplicative scheduled and unscheduled production of integrated scientific and technical and general military intelligence for all DOD intelligence components.

(d) Establishing and maintaining a DOD-wide system of DODIPP.

(e) Supporting the DOD weapons acquisition process by producing threat assessments within DIA (or validating assessments produced by other DOD intelligence components) for all major DOD acquisition programs.

(f) Establishing and conducting research, development, test, and evaluation programs and projects to accomplish the DIA mission.

(g) Managing the execution of the Foreign Materiel Program, except for those acquisition and exploitation activities for which NSA and USD(I) have primary responsibility.

(h) **Armed Forces Medical Intelligence Center.** AFMIC, located at Ft. Detrick in Frederick, Maryland, is **the only Tri-Service medical intelligence organization within the USG.** AFMIC products are tailored to the unique requirements of deployed operational forces but are also widely used by national-level policymakers and the acquisition community. Mission responsibilities include the production of finished, all-source, medical intelligence in support of DOD and its components, national policymakers, and other federal government agencies. Assessments, forecasts, and databases are prepared on foreign military and civilian health care capabilities and trends, worldwide infectious disease occurrence, global environmental health risks, militarily significant life science technologies, and foreign BW programs to include dual-use biotechnology.

(i) **Missile and Space Intelligence Center.** MSIC, located at Redstone Arsenal near Huntsville, Alabama, **provides current and comprehensive scientific and technical intelligence to US decision makers, weapon system developers, and combatant commanders**. It develops and disseminates intelligence concerning the threat from offensive and defensive guided-missile systems, directed-energy weapons, selected space programs and/or systems and related command, control, and communications (C3) to support operationally deployed forces and the materiel acquisition process. Additionally, it develops and distributes digital threat simulations to force developers and operational forces.

(3) **Directorate for MASINT and Technical Collection.** DT **manages collection requirements and operations** and ensures the effective acquisition and application of all-source intelligence collection resources to satisfy DOD collection requirements. DT also provides a broad range of MASINT support to joint operations, and national, strategic, and non-DOD customers. DT operates the MOCC, located in the NMJIC, to ensure that time-sensitive MASINT requirements of commanders are met. Additionally, MASLOs provide assistance to the combatant commanders for MASINT products. DT performs the following functions:

(a) Provide responsive MASINT support to the IC, DOD, NSC, and other USG departments and agencies.

(b) Manage MASINT for the NFIP and DOD.

(c) Manage all appropriate research and development activities related to MASINT tasking, collection, processing, exploitation, and dissemination.

(d) Through a central MASINT tasking authority, task national MASINT collection assets of the IC and DOD.

(e) Establish and maintain a national MASINT requirements system.

(f) Coordinate MASINT exploitation activities among diverse national and DOD organizations.

(g) Advise the DCI and the Secretary of Defense on the adequacy of existing and potential systems to satisfy requirements for national and nonnational MASINT.

(h) Develop and implement standards and architectures to foster equipment interoperability and training associated with MASINT tasking, collection, processing, exploitation, and dissemination.

(i) Ensure that MASINT systems participate in exercises involving support to US military forces.

(j) Develop, recommend, and implement policy regarding MASINT tasking, collection, processing, exploitation, and dissemination.

(k) Validate, register, and recommend priorities for military intelligence requirements; assign collection responsibilities; and monitor the application of DOD collection resources to such requirements.

(l) Oversee the development, procurement, and operation of military intelligence collection systems funded in the GDIP, and develop recommendations for future systems.

(m) Implement national intelligence collection tasking authority after such authority is transferred from the DCI to the Secretary of Defense in crisis and/or conflict situations.

(n) Serve as the Collection Fund Manager to ensure funding and manpower for valid joint resource requirements.

(4) **Directorate for Human Intelligence (DH). DH conducts HUMINT management and operations worldwide in response to DOD and combatant command requirements.** The Directorate provides global reach and persistent access to worldwide collection targets by providing a range of HUMINT capabilities tailored to meet the needs of its customers, from official military-to-military intelligence exchanges to unilateral operations. DH directs all nontactical DOD HUMINT activities through the DHS. In addition to providing HUMINT collection support, the DHS deploys a forward HSE to each combatant command to provide a conduit for coordination with the DHS, to ensure the J-2 is fully informed of the DHS activities, and to assist the command in obtaining HUMINT support. HUMINT operating bases and locations around the world also satisfy joint information requirements. The DHS provides HUMINT resources in response to joint force requirements which may include augmenting a joint force J-2 CI/HUMINT staff element and/or HUMINT operations cell and deploying special collection teams. The DHS also manages the worldwide Defense Attaché System. Defense attachés observe and report military and political-military information of interest to the Joint Staff, Services, DOD, and combatant commands.

(5) **Directorate for Information Management and Chief Information Officer (DS).** DS provides information systems and services to the IC in support of warfighters, national policymakers, and defense acquisition authorities. Its functions include information systems and communication engineering development, integration, and operations for DIA and the IC; information library services, hardcopy and electronic publication and dissemination; video and visual information services; GDIP intelligence infrastructure functional management; and DODIIS planning, engineering, and life-cycle management efforts. Additional responsibilities include the following:

(a) Overseeing the research and development, procurement, and operation of DOD intelligence infrastructure-related programs, systems, and activities funded in the GDIP, to include printing, processing, communications, and information systems.

(b) Providing centralized intelligence dissemination services and supervising a DOD-wide intelligence dissemination system.

(6) **Directorate for External Relations (DX).** DX, located in the Pentagon, is responsible for ensuring that all requirements for military intelligence support to the Secretary of Defense, senior DOD policymakers, and members of Congress are satisfied. DX routinely interfaces with the IC, the Services, the combatant commands and substantive analysts in bringing together intelligence-policy perspectives. DX is the central authority for all DOD activities related to non-SIGINT and non-IMINT intelligence agreements and arrangements with foreign governments, allies, and international organizations. It also serves as the single authority for all disclosures of DIA information to foreign governments and international organizations. DX's Defense Intelligence Liaison Offices interface with the Commonwealth nations (Canada, Australia, and the United Kingdom) in the sharing of intelligence impacting on joint operations. DX serves as the single point of contact in DIA for requests from members of Congress and congressional committees. Additionally, DX manages the DISOs assigned to the combatant commands, US Forces Korea, Supreme HQ Allied Powers Europe, NATO HQ, and Allied Forces Southern Europe HQ. DX is also responsible for critical infrastructure protection activities related to ISR resources and is a focal point for DIA Homeland Security policy issues.

(7) **Directorate for Administration (DA). DA develops and implements DIA personnel management policies, procedures, and programs.** DA supports Agency missions for training and career development of personnel and manages support services in the areas of engineering, logistics, travel, space management, and facilities maintenance.

(a) DA operates the Joint Military Intelligence Training Center (JMITC). JMITC provides strategic and joint intelligence training in resident and nonresident modes to DIA, the combatant commands, the Military Services, other DOD components, and other federal agencies. It also provides DOD-wide oversight of general intelligence training, functional management for GDIP-funded intelligence training, and validation of DOD general intelligence training requirements.

(b) Within DA, the Counterintelligence and Security Activity (DAC) manages security and CI programs to safeguard DIA personnel, information, facilities, systems, and operations. This includes operating as the focal point for all joint CI issues arising from or in support of the Chairman of the Joint Chiefs of Staff and combatant commanders, and serving as the coordination point among Joint Staff directorates and the Service CI elements. It provides CI analysis, production, and staff support to OSD, the Chairman of the Joint Chiefs of Staff, combatant commands, Defense agencies, DOD special activities, and the national IC for assigned regions. DAC also serves as the manager for all DID CI collection, production, and operations requirements, implements SCI security policy within DOD, and develops and publishes security policy manuals, regulations, and handbooks for DOD. The overseas branch provides tailored technical security support and monitors the threats to the security of US customers.

(8) **Joint Military Intelligence College.** The College, located at the DIAC, educates military and civilian intelligence professionals. A regionally accredited institution, the College is authorized by Congress to award two degrees, the Master of Science of Strategic Intelligence and the Bachelor of Science in Intelligence. Its educational programs prepare military and civilian personnel for command, staff, and policymaking positions. The College manages an

intelligence research program that conducts and disseminates relevant academic research on topics of significance to present and future intelligence missions.

6. National Security Agency/Central Security Service and the United States Cryptologic System

The NSA/CSS is a unified organization structured to protect the security of US signals and information systems and provide intelligence information derived from the exploitation of the signals and information systems of America's adversaries. The NSA/CSS has a unique position among the defense agencies because of its government-wide responsibilities providing products and services to the DOD IC, government agencies, industry partners, and select allies and coalition partners. NSA/CSS is also designated as a Combat Support Agency performing 22 specific combat support activities for DOD.

a. The CSS was established to promote a full partnership between the NSA and the cryptologic elements of the Armed Forces. By combining NSA and CSS, a more unified DOD cryptologic effort is provided. The CSS is composed of the SCEs of the US Military Services.

b. The USCS is a term used to describe the USG entities tasked with collecting and exploiting SIGINT and with preserving the availability, integrity, authentication, confidentiality, and nonrepudiation of information systems. The NSA/CSS manages cryptologic planning and operations in support of the USCS. As the Community Functional Lead for SIGINT, the Director, National Security Agency (DIRNSA) is responsible for the overall management and operational control of the USCS.

c. NSA/CSS has two core missions: SIGINT and information assurance (IA).

(1) SIGINT comprises either individually or in combination all COMINT, ELINT, and Foreign Instrumentation Signals Intelligence.

(2) IA encompasses the disciplines and activities that ensure the availability, integrity, authentication, confidentiality, and nonrepudiation of national security information. To meet management, readiness and operational responsibilities, NSA/CSS performs the following functions:

(a) Management

1. Exercise SIGINT operational control over the USCS and execute the responsibilities of the Secretary of Defense as Executive Agent for US IA and interagency operations security (OPSEC) training.

2. Functions as the SIGINT and IA advisor to the Secretary of Defense, the DCI, the Chairman of the Joint Chiefs of Staff and the Joint Staff. Provides cryptologic advice and assistance to the combatant commands and other military commands through collocated NSA/CSS representatives.

3. Determines, in conjunction with the combatant commanders, when the DIRNSA should delegate SIGINT operational tasking authority.

4. Implements programs and initiatives that promote interaction among national and tactical cryptologic assets.

5. Functions as the National Manager for National Security Telecommunication and Information System Security.

(b) Readiness

1. Responds directly and quickly to the validated and prioritized readiness information requirements.

2. Ensures that designated wartime and contingency cryptologic resources are adequate to support readiness requirements.

3. Provides security assessments to assist in determining the vulnerability of national security systems.

4. Assists in developing IA capabilities; evaluating and developing national security system architectures and standards; managing associated encryption systems; and designing secure Internet architectures, standards, and protocols.

5. Assists in defining national security systems transmission security standards.

6. Evaluates jam-resistant, low-probability-of-interception, and other detection systems.

7. Develops, tests, and implements new concepts, plans, capabilities, and procedures to improve cryptologic support functions.

8. Provides systems development, engineering, and programmatic support to national or multinational cryptologic initiatives.

9. Ensures the technical adequacy of all cryptologic training.

10. Conducts, participates in, and supports both US and allied exercises to facilitate use of cryptologic resources.

(c) Operations

1. Provides information systems encryption materials during peacetime, in crisis, contingency, and war.

2. Provides cryptologic support to IO.

3. Integrates US and allied cryptologic activities.

4. Supports, in coordination with other national intelligence activities, US contingency operations consistent with procedures defined in CJCSMs for support to conventional and special operations missions.

5. Supports special technical operations.

6. Provides SIGINT and IA support through appropriate channels to the commanders responsible for C2 of mobile SIGINT platforms.

7. Provides direct and dedicated interoperable cryptologic communications support to facilitate the delivery of perishable SIGINT and provides for continued cryptologic support to emergency or rapid recovery and reconstitution teams.

d. **Organizational Framework for Cryptologic Support.** NSA/CSS provides cryptologic support to departments, agencies, commands, and other USG activities and provides expeditious responses to user information needs. The USCS is responsive to the needs of all authorized cryptologic users, including military commanders for whom special support arrangements have been devised as part of the system. The following are the mechanisms that support departments, agencies, commands, and other USG activities:

(1) **National Security Operations Center.** The NSOC is DIRNSA's cryptologic mission management center for USCS time-sensitive SIGINT and IA operations. It continuously monitors world events and the status of the USCS, and manages the NSA/CSS mission in real time. The NSOC also directly supports activities required for mission execution.

(2) **Special Support Activity (SSA).** The SSA provides real time threat warning in its role as the contingency and crisis management center of the NSOC. It serves as the NSA/CSS lead on all NISTs, and its personnel are deployable for up to 90 days. It may function as a temporary CSG in responding to RFIs by commanders, and also monitors exercises.

(3) **Regional SIGINT Operations Centers (RSOCs).** RSOCs are NSA field activities with the mission to enhance SIGINT support to commanders at all echelons. The RSOCs are regionally focused and receive inputs from multiple sources. These centers are multi-Service military and civilian facilities and provide an opportunity to build on the synergy of national and tactical assets.

(4) **NSA/CSS Representatives.** NCRs are senior representatives of the DIRNSA, accredited to the combatant commands, other senior military commands, and the DOS and DOD. The NCRs at the combatant commands are the senior cryptologic authorities in the region and are the special advisors to the combatant commander for cryptologic matters.

(5) **Cryptologic Services Groups.** The CSGs are extensions of the NSOC and are the primary mechanism for the supported organization to gain entrance into and support from the USCS. CSGs provide cryptologic advice, and assistance. They advise organizations of USCS capabilities and limitations that might affect its cryptologic requirements and recommend to NSA/CSS those actions necessary to ensure cryptologic responsiveness.

(6) **The Joint COMSEC Monitor Activity (JCMA).** JCMA is a JCS-sponsored organization operating under the auspices of the NSA. The mission of the JCMA is to conduct COMSEC monitoring (collection, analysis, and reporting) of DOD telecommunications signals (encrypted and unencrypted) and automated information systems and monitoring of related noncommunications signals. The purpose is to identify vulnerabilities exploitable by potential adversaries and to recommend countermeasures and corrective actions.

(7) **National Intelligence Support Team.** Based on lessons learned from Operations DESERT SHIELD and DESERT STORM, all national-level agencies combined their separately deployed intelligence support teams into one NIST. The NIST concept was designed to create a dynamic flow of information and intelligence to and from the operational area. The intent of the NIST is to provide decision makers timely and tailored intelligence. The NSA element of the NIST brings a wide range of services, which include analytic support and secure voice and/or data connectivity to supported organizations via the NSOC. As a crisis matures into a sustained operation, the NIST is often dissolved and replaced by a combatant command's or Department's organic intelligence support apparatus to include a CSG.

(8) **NSA/CSS Customer LNOs.** NSA/CSS customer LNOs act as representatives to customers that do not have an assigned NCR. LNOs are provided to various Executive Branch agencies, such as the Departments of Justice and Commerce, which use SIGINT product, but not on the scale of Defense or State.

(9) **Support to the Department of Defense and the Joint Chiefs of Staff.** DIRNSA is the principal cryptologic advisor to both the Secretary of Defense and the Chairman of the Joint Chiefs of Staff, keeping both fully informed on cryptologic matters. In additional to the national cryptologic representative defense (NCRDEF) who provides day-to-day advice and support to the DOD, the DIA, the JCS, and the Military Departments, the Joint Staff CSG provides the JCS with time-sensitive cryptologic services. Additionally, both the NCRDEF and Joint Staff CSG provide NSA/CSS with advance warning and advice on DOD policies, Joint Staff plans, and IA and intelligence requirements.

e. While many NSA systems could have useful applications in contingency operations, the most commonly employed systems are TRIBUTARY and Critical Source (CS). Though not exclusive to NIST deployments, these systems are most often deployed with NISTs.

(1) **TRIBUTARY.** The TRIBUTARY System is a voice and limited data network that can provide direct real-time threat warning intelligence information to operational forces. The TRIBUTARY System uses portable UHF satellite communications (SATCOM) equipment

to provide military commanders with direct subscriber linkage to the NSOC SSA. Commanders can access one of the SSA's standing TRIBUTARY networks with most any organic UHF SATCOM system by simply requesting satellite frequencies and cryptographic materials. NSA provided TRIBUTARY equipment includes an LST-5 UHF radio and an antenna appropriate for the mission. A portable computer with a SATCOM modem is deployed as required to support data requirements. Within four hours of a request, a two-man SSA team with TRIBUTARY access and equipment can be activated and deployed to assist a commander at any level in response to a crisis or contingency. Although the main purpose of TRIBUTARY is to provide time-sensitive threat warning and reporting, the voice and data capabilities can also be used to support the initial functions of a NIST until a CS is deployed. If required, SSA can establish a separate dedicated network to support threat-warning requirements in a sensitive OPSEC environment.

(2) **Critical Source.** CS is a scaleable, deployable equipment suite that provides operational forces with access to theater and national SIGINT support and other national intelligence resources. This secure, multimedia, tactical voice and data processing system extends the powerful NSA/CSS communications infrastructure to a forward-deployed CSG or the NSA element of a NIST. Within 72 hours of request for support, NSA can provide either "heavy" or "light" CS to contingency operations worldwide for full reach back, secure communications to Washington-area intelligence agencies. The CS deploys with its own satellite dish and base band secure communications suite. The "heavy" system is comprised of a vehicle-mounted full communications center package with organic SATCOM. The "light" system provides access to the same national-level networks; however, it is smaller, more compact and can be deployed in containers that are transportable on one US Air Force standard pallet. These systems are regularly deployed to support NIST communications requirements and provide entry into the NSTS or "Gray phone" and other secure networks. Communications pathway (bandwidth) and logistic support to the deployed CS are the responsibility of the supported command.

f. Support to military operations depends on JWICS and on the SIPRNET, the DODIIS-standard SECRET-level-high-speed communications and dissemination network. The NRT dissemination (NRTD) system, one of NSA's key combat support mechanisms, depends upon JWICS and SIPRNET for Internet Protocol (IP) network broadcast of vital time-sensitive data. NRTD uses satellite broadcast media for delivery of intelligence to combat units not connected to the IP networks (JWICS or SIPRNET).

7. National Geospatial-Intelligence Agency

NGA is both an IC organization and a DOD combat support agency whose mission is to provide timely, relevant, and accurate geospatial intelligence in support of national security. To do so, NGA capitalizes on all forms of what is traditionally categorized as imagery, imagery intelligence, and geospatial data and information — now known as geospatial intelligence to provide the foundational "knowledge map" in support of national intelligence analysis.

a. **Responsibilities.** NGA provides GEOINT and services to national decision makers, military commanders, the IC, and other USG entities, as appropriate. The Director of NGA advises the DCI, Secretary of Defense, Chairman of the Joint Chiefs of Staff, and the combatant

commanders on all issues related to geospatial intelligence. This support extends to the departments and agencies of the Federal government to the extent allowed by law. The Director of NGA also serves as functional manager for the National System for Geospatial Intelligence (NSGI).

b. **Organization.** NGA is organized to ensure support for current requirements while simultaneously facilitating the transformation necessary to fulfill the geospatial intelligence mission (see Figure B-6).

(1) NGA is composed of an Executive Leadership Group, Staff Offices, and Directorates. The Executive Leadership Group is the senior corporate body and provides leadership direction for NGA's internal and external activities.

(2) Several NGA Staff Offices provide essential support for military operations. This support includes:

(a) Managing and tasking national imagery collection operations on behalf of the DCI to include the integration of national, NGA-purchased commercial, and selected airborne collection requirements.

(b) Developing and disseminating geospatial intelligence policy and guidance on behalf of the DCI and the Secretary of Defense. NGA also develops and implements geospatial intelligence release and disclosure policy.

(c) Providing planning and programmatic guidance to the members of the NSGI for geospatial intelligence programs and activities.

(d) Developing, negotiating, and managing international agreements for geospatial intelligence data sharing and co-production with foreign partners.

(3) Five of NGA's Directorates are considered line organizations:

(a) Analysis and Production Directorate: Provides geospatial intelligence analysis and production to meet customer requirements.

(b) Source Operations and Management Directorate: executes the nation's end-to-end space-based, airborne, and commercial imagery requirements for geospatial intelligence.

(c) Enterprise Operations Directorate: Responsible for day-to-day systems operations and leveraging technology to ensure and protect NGA's mission by operating the NSGI and providing enterprise, corporate, dissemination and information services.

(d) Acquisition Directorate: Plans and implements acquisition of geospatial intelligence systems for the NSGI.

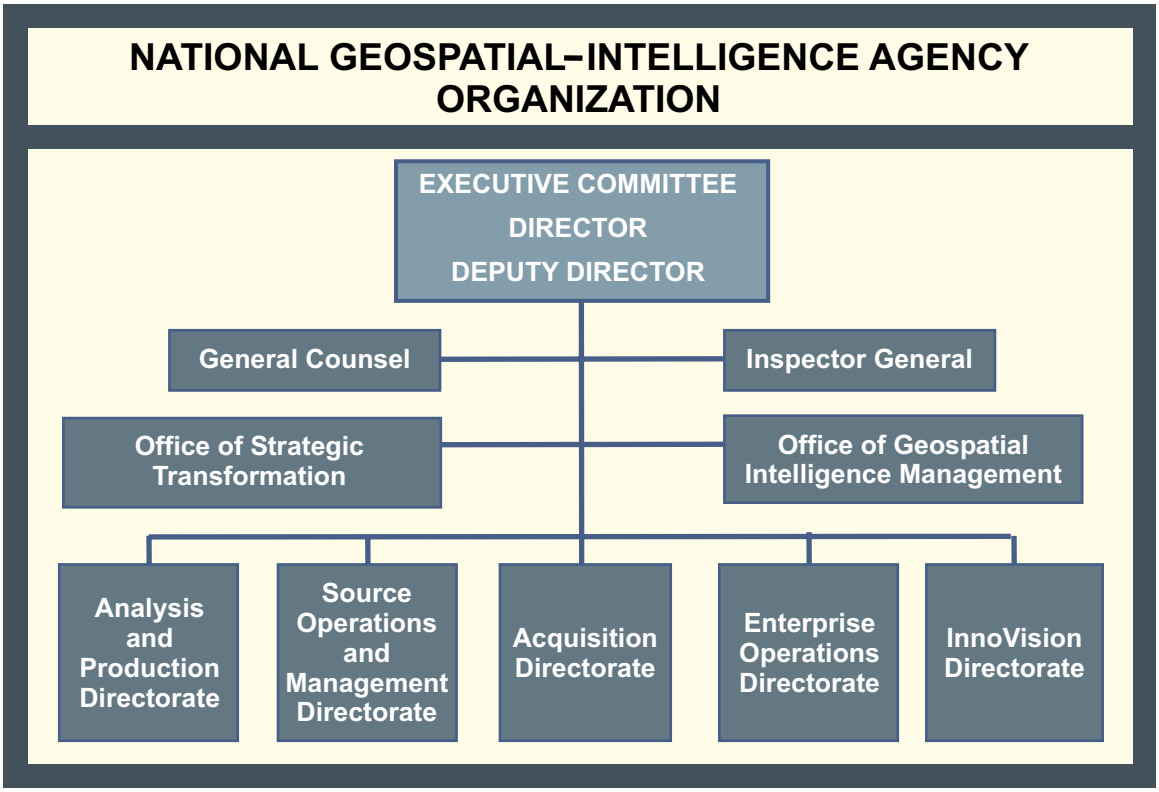


Figure B-6. National Geospatial-Intelligence Agency Organization

(e) InnoVision Directorate: Forecasts environments, defines future needs, and develops innovative solutions and technologies through focused research and development and systems engineering.

(4) The remaining Directorates, the enabling organizations, and staff offices provide specialized support for NSGI community activities, including:

(a) Beginning, intermediate, and advanced geospatial and imagery analysis training to NGA, the Services, and the IC through the National Geospatial Intelligence College.

(b) Provide on-site training support for geospatial intelligence systems and procedures through mobile training teams. Though these teams typically train during peacetime, they often deploy during crisis situations.

(c) Provide program guidance to the NSGI.

(d) Provide geospatial intelligence support to deployed customers, and support deployed NGA support teams.

c. **NGA Support to Military Operations.** NGA provides geospatial intelligence to support military planning, decision making, targeting, and intelligence production during peacetime and crisis. This support includes:

(1) Imagery exploitation. NGA exploits all forms of traditional and nontraditional data, from national, civil, and commercial sources.

(2) Provide traditional and specialized hardcopy geospatial products and electronic data.

(3) Provide safety of navigation products and services.

(4) Populate and maintain national databases that provide the visualization and analytical framework to support decision making.

(5) Manage the acquisition of commercial and foreign government remote sensing data for DOD users.

(6) Maintain crisis-specific geospatial intelligence products and data on NGA's JWICS and SIPRNET systems to complement its direct support activities.

d. **NGA Customer Support.** The NST is the primary mechanism for NGA interaction with its customers. The NST coordinates NGA's operational, policy and training support to its customers.

(1) NGA maintains NSTs at the Joint Staff, combatant commands, Services, and National and Defense agencies. Additional NSTs are located at several non-DOD government organizations (e.g., Department of State). A typical NGA NST at the combatant commands and Service headquarters is composed of a senior representative (military O-6 or GS-15), staff officers, and imagery and geospatial analysts. A reach back component at NGA Headquarters focuses NGA production support.

(2) In addition to using NSTs, NGA may deploy crisis support teams of two to five imagery and geospatial analysts upon request, either independently, as augmentation to an existing NST, or as part of a NIST. These teams of government and/or contract personnel employ deployable geospatial intelligence production systems. NST personnel can reach back to NGA for data and products, fuse this information with tactical and theater sources, and work with users to produce products tailored to their needs.

8. National Reconnaissance Office

The mission of the NRO is to enhance USG and military information superiority, across the range of military operations. The NRO is responsible for the application of unique and innovative technology, large scale systems engineering, development and acquisition, and operations of space reconnaissance systems and related intelligence activities.

a. **Organization.** The NRO's organizational structure is shown in Figure B-7. The position of Deputy Director for Military Support (DDMS) was created in 1990 when the role and value of NRO systems to support military operations was recognized. The DDMS is responsible for consolidating

NRO military support and oversees all actions impacting the DOD. NRO directorates and offices provide NRO training, education, and exercise support to national, military, and civil customers. The NRO's support to military programs includes tailored training, professional military education, and exercise support conducted by the Operational Support Office and the IMINT and SIGINT Directorates. The Plans and Analysis Office develops engineering assessments of future military requirements to ensure that they can be met by systems being launched today.

b. **Responsibilities.** NRO responsibilities include support to I&W, monitoring arms control agreements, and crisis support to the planning and conduct of military operations. The NRO accomplishes its mission by building and operating reconnaissance satellites and associated communications systems. The NRO LNOs and theater support representatives located with each of the combatant commands serve as direct links to NRO for the combatant commanders and their staffs.

c. **Application of Data.** NRO support must be continuously incorporated into the planning process. As a key element in achieving information superiority, it should be viewed as part of all aspects of full spectrum dominance, not simply those areas that fall within the purview of the joint force J-2. Many of the greatest gains can be realized in nontraditional areas such as supporting logistics with terrain data from NRO systems or providing warning for force protection. The NRO accommodates the functional needs of battlespace information dominance with near-continuous coverage architectures in partnerships with the OSD, JCS, IC, and USSTRATCOM. Advances in technology enable the NRO to provide greater amounts of useful information to ever lower

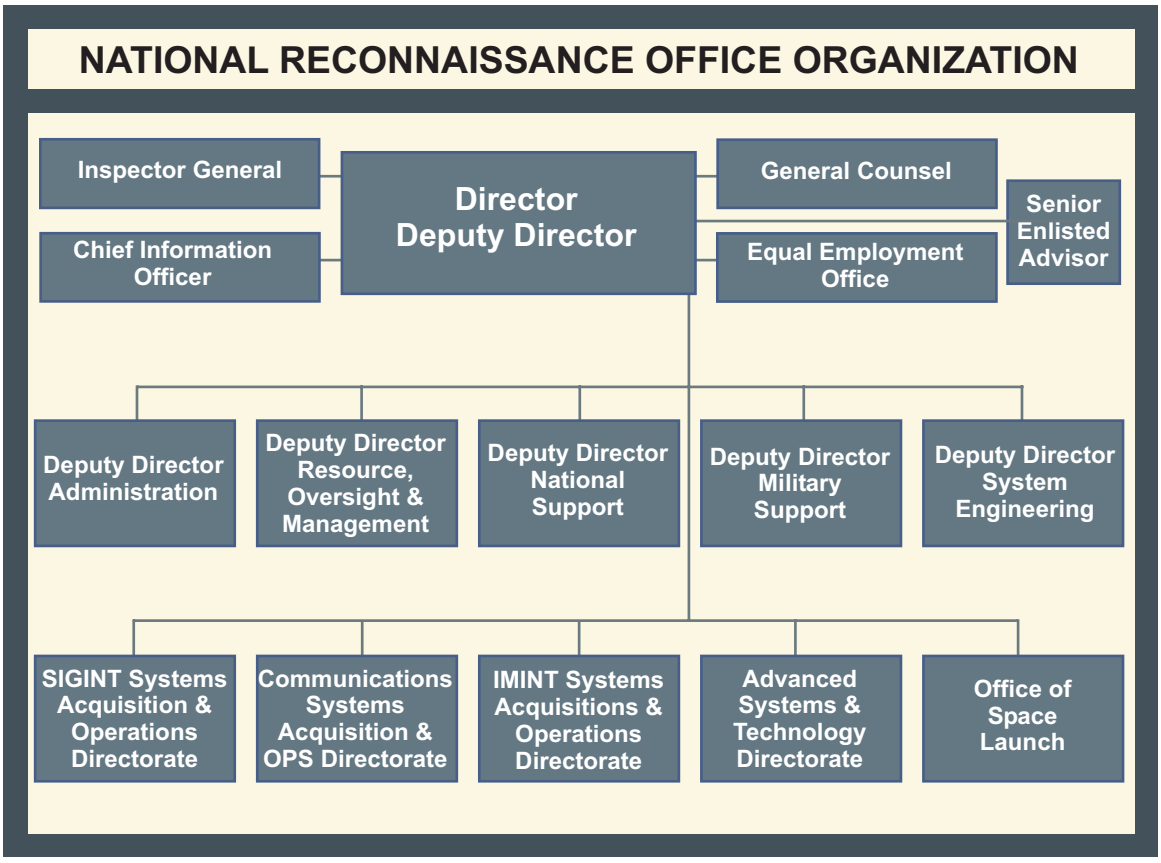


Figure B-7. National Reconnaissance Office Organization

tactical echelons, with the primary impact of NRO data being realized at the operational level. With regard to security, the goal is to downgrade classification and disseminate products essential to operations.

d. **Obtaining Support.** The DIA is the overall coordinator of NRO support for DOD, which it manages with on-line systems. IMINT requirements are tasked through NGA, SIGINT requirements through NSA, and MASINT requirements through DIA. NRO LNOs and the NRO's Operational Support Office facilitate end-to-end support from education and tasking to dissemination of the product and service. The basic reference for obtaining support is the Joint Tactical Exploitation of National Systems Manual.

9. Service Intelligence Organizations

The Chiefs of the Military Services provide intelligence support for Departmental missions related to military systems, equipment, training, and national intelligence activities. The Services act to support DOD entities, including combatant commands and the Service components of those commands.

a. **US Army**

(1) **Deputy Chief of Staff (DCS) for Intelligence, G-2.** The Army G-2 is responsible to the Chief of Staff, Army for long-range planning and policy guidance on all matters relating to Army intelligence, security, and CI activities. The G-2 manages the Army portion of the NFIP, Army departmental-level general military intelligence and scientific and technical intelligence production missions, intelligence readiness training, the Army language program, and the Army Foreign Material Program. The G-2 exercises staff supervision over the US Army INSCOM and has operational control over its departmental production resources.

(2) **INSCOM.** INSCOM, headquartered at Fort Belvoir, Virginia, is an operational HQ responsible for Army echelons above corps (EAC) intelligence and electronic warfare (IEW) operations executed by its subordinate commands located worldwide. INSCOM is a major participant in national intelligence activities and support to theater IEW operations. Its subordinate commands consist of three broad categories of organizations that provide cryptologic, general military, and theater intelligence support to strategic and operational level commanders in the areas of TIARA HUMINT, IMINT, MASINT, SIGINT, CI, IO, and intelligence analysis and/or production. Through its theater MI brigades and other special mission units, INSCOM:

(a) Provides direct support operational intelligence units to Army component commanders.

(b) Conducts overt TIARA HUMINT collection worldwide in response to Army commanders' requirements.

(c) Performs ground MASINT collection for the Defense IC, under the direction of the Defense Intelligence Agency Directorate for MASINT and Technical Collection, in support of theater, Army, and national requirements.

(d) Functions as the Army's SCE for the US SIGINT System and provides support to NSA cryptologic missions with Army SIGINT units located at NSA HQ and the regional SIGINT operations centers.

(e) In coordination with the FBI in CONUS and the CIA OCONUS, conducts CI investigations of and operations against foreign organizations and persons which target US Army personnel and equipment by means of espionage, sabotage, or terrorist activities.

(f) Performs CI analysis and production for the Army.

(3) **Theater MI Brigades and/or Groups.** INSCOM theater MI brigades and/or groups conduct multidiscipline EAC intelligence operations in support of the respective theater's Army component commander and, if one is designated by the JFC, the joint force land component commander (JFLCC). The four EAC units are:

(a) 66th MI Group, US Army Europe, USEUCOM.

(b) 500th MI Group, US Army Pacific, US Pacific Command.

(c) 501st MI Brigade, 8th US Army, US Forces Korea.

(d) 513th MI Brigade. The 513th is tasked to provide support, as required, to Army forces (ARFOR) commanders in USEUCOM, US Central Command, and US Southern Command.

(e) 704th MI Brigade, Ft. Meade, Maryland.

(4) **902d MI Group**

(a) The 902d MI Group, located at Fort Meade, Maryland is subordinate to INSCOM and is the largest CI organization within the Department of Defense. The Group has a worldwide mission to detect and neutralize foreign intelligence collection against the US Army's forces, operations, and technologies. This encompasses both offensive and defensive CI operations and counterespionage (CE) investigations, to include investigations of Army information network denial and/or disruptions, computer systems penetrations, and attempted penetrations. In this regard, the Group supports the Army's 1st Information Operations Command (Land) (1st IOC (Land)) C2 protection mission through its investigations, analysis, and CI operations. The Group has supported numerous JTFs with tailored CI support packages, to include operations in Somalia, Haiti, Bosnia, Europe, and Central America. It conducts RED team evaluations to provide a realistic picture of a command's organizational vulnerabilities. The Group also provides CI support to the Army technology base and acquisition community.

(b) The 902d MI Group is one of three DOD CONUS-based units chartered to identify and report Foreign Intelligence Service (FIS) collection operations (i.e., threat information, modus operandi, interests, habits, trends, activities). Analysts at the Group's Army CI Center (ACIC) support US Army CE investigations, CI operations, C2 protection and special access programs through analysis of FIS targets, trends, and modus operandi; provide analysis of raw information and open-source material to meet worldwide Army requirements; and produce multidiscipline CI threat assessments, counterterrorism, and other threat products. It is the ACIC that conducts the Army CI production mission to complement the NGIC.

(c) The 902d MI Group is the Army's sole element responsible for providing SCI oversight, inspections, advice, and assistance and site-based accreditation for the Army component of the DODIIS computer security programs. Through its battalions, the Group identifies and neutralizes technical penetrations directed against US forces, secrets, and technology through its technical surveillance countermeasures (TSCM) and TEMPEST teams; conducts polygraph examinations in support of Army technology and operations; and provides signals profiling primarily for sensitive facilities and US Army SOF. The 902d MI Group provides basic TSCM training for all DOD personnel and is the only TSCM certification-granting institution in the Army.

(d) The 902d MI Group conducts CI operations to determine foreign collection patterns and areas of interest; predicts foreign technology collection requirements; and develops cost effective countermeasures that will prevent those targeted critical technologies from being defeated on the battlefield, countered, or duplicated to the detriment of US forces. The 902d MI Group addresses the foreign collection threat posed by foreign LNOs, foreign scientist and engineer exchange programs, foreign visitor programs, and the data exchange programs as well as the emerging CI threat to the Army from other nontraditional sources.

(e) The 902d MI Group provides direct CI support to the Army Special Operations Command, DTRA, NGA, and the combatant commands and subordinate forces. The group conducts national-level liaison for INSCOM.

(5) **National Ground Intelligence Center.** The NGIC, located in Charlottesville, Virginia, is assigned to INSCOM and is under the operational control (OPCON) of the Army G-2. NGIC is the Service National production center for ground forces intelligence and has DODIPP primary production responsibility for most ground force intelligence functional codes. The NGIC provides the following:

(a) All-source scientific, technical, and general military intelligence on foreign ground forces in support of Army Title 10 requirements.

(b) IMINT and secondary imagery dissemination to support training, exercises, and contingency planning.

(c) Executes the Army's foreign materiel acquisition requirements and exploitation program.

(d) Current- and future-oriented ground capabilities threat assessments to support operational forces, the combat and materiel development community, contingency planners, force planners, wargame personnel, and doctrine development organizations.

(e) Detailed analysis and production of systems capabilities and parametric data for all foreign ground and ground-related systems (to include helicopters, air defense guns, infantry, armor and anti-armor, fire support, engineer, mines, EW, reconnaissance, chemical warfare, TIM with potential dual-use capability, directed-energy weapons, and C3 systems). Produces assessments of ground systems trends.

(f) A shared production and database maintenance responsibility for selected countries.

(g) Reinforcing support to other intelligence centers as required.

(6) **1st Information Operations Command (Land).** 1st IOC (Land) is assigned to INSCOM and is under the OPCON of the Army DCS, component operations staff officer [G-3]. The 1st IOC (Land) provides operations support for the planning and execution of the IO portion of a campaign from the Military Department level through tactical-levels. Support across the spectrum of IO is also provided to the JFLCC, if one is designated by the JFC. Primary 1st IOC (Land) functions include the following:

(a) Provide IO staff support to ARFOR and JFLCC staff.

(b) Coordinate IO intelligence and CI support to operational and tactical ground commanders, including the JFLCC.

(c) Coordinate and deploy field support teams to assist ARFOR commanders and JFLCCs in the area of C2-protect, C2-attack and C2-support planning.

(d) Develop and sustain rapid response capabilities and oppose penetrations of Army C4I systems and processes.

b. **US Navy**

(1) **Director of Naval Intelligence.** DNI is the intelligence executive to the Chief of Naval Operations (CNO), exercising overall authority throughout the Department of the Navy on matters pertaining to intelligence, cryptology, CI, and special security. The DNI manages the Navy portion of the national foreign intelligence, sets naval intelligence policy, and directs naval intelligence planning and programs.

(2) **Office of Naval Intelligence.** The Commander of ONI, headquartered at the National Maritime Intelligence Center at Suitland, Maryland, provides the Department of the Navy the intelligence necessary to plan, build, train, equip, and maintain US maritime forces.

(3) **National Maritime Intelligence Center. The NMIC is the national production center for maritime intelligence.** Located at Suitland, Maryland, NMIC consists of ONI, a detachment of the MCIA, USCG ICC, and the NIWA. The NMIC supports Navy, Marine Corps, Coast Guard, joint, and national-level requirements through a variety of intelligence production capabilities, including:

(a) Naval weapons systems analysis.

(b) Integrated tactical analysis of foreign navies and maritime threats.

(c) Acoustic collection and analysis.

(d) Naval foreign material acquisition and exploitation.

(e) Civil maritime analysis of topics such as merchant shipping, sanctions violations, commercial treaty violations, counterdrug, and maritime smuggling.

(f) Intelligence support to naval IO.

(g) Naval-related collection and information systems development.

(h) Community management support on naval budget, security, and reserve issues.

(4) **Naval Security Group.** Commander, Naval Security Group (CNSG) Command, is located at Fort Meade, MD. CNSG reports directly to the CNO as an echelon II command, and is a principal assistant to DNI. CNSG provides technical guidance and support to cryptologic and IO activities of US Navy operating forces.

(5) **Naval Criminal Investigative Service. NCIS fulfills the criminal investigative and CI responsibilities of the Navy.** The Director, NCIS, is directly subordinate to the Secretary of the Navy, and also serves as Assistant Director of Naval Intelligence for CI. Intelligence on potential terrorist and UW threats to the Navy and Marine Corps is provided by the Multiple Threat Alert Center (MTAC), a 24-hour terrorism I&W center. A branch of NCIS, the MTAC provides a full range of counterterrorism, CI, and technology transfer analysis and production for the Department of the Navy.

c. **US Air Force**

(1) **Air Force Director of Intelligence, Surveillance, and Reconnaissance.** AF/XOI is responsible to the Air Force Chief and Deputy Chief of Staff for Air and Space Operations for policy, planning, programming, resource allocation, and program evaluation activities aimed at ensuring information superiority in peace, crisis, and war.

(2) **Air Intelligence Agency.** AIA, subordinate to Air Combat Command and headquartered at Lackland Air Force Base (AFB), Texas, **oversees processing and production**

elements worldwide. It provides customers at all echelons with multi-source intelligence products, applications, and services and provides intelligence expertise in the areas of IO (to include information protection), acquisition, foreign weapons systems and technology, and treaty monitoring. Additionally, AIA serves as the Air Force Validation Office for Production and Application Requirements under the DODIPP. When Air Force component intelligence requirements exceed the theater's capabilities, AIA may reinforce the combatant command with analytical expertise and products.

(3) **National Air and Space Intelligence Center. NASIC, subordinate to AIA, is the principal agency for assessing the foreign air and space threat.** NASIC can provide deployed forces with unique capabilities for aerospace intelligence for DOD operational commands, research and development centers, weapon acquisition agencies, and national planners and policymakers. HQ NASIC is located at Wright-Patterson AFB, Ohio; subordinate NASIC elements operate in Washington, DC, Langley AFB, Virginia, and Offutt AFB, Nebraska.

(4) **Air Force Information Warfare Center. AFIWC explores, applies, and migrates offensive and defensive information warfare (IW) capabilities** for operations, acquisition, and testing. AFIWC provides advanced IW training for the Air Force, develops and maintains command and control warfare (C2W) databases and applications, provides vulnerability analyses of friendly electronic systems, and protects friendly C2 against adversary attacks. AFIWC's databases and applications are major dissemination mechanisms that provide IW-related intelligence to the warfighter. Support is provided directly from AFIWC and JIOC which are collocated in San Antonio, Texas. (See Annex A, "Joint Centers").

(5) **Air Force Office of Special Investigations. AFOSI** is responsible to the US Air Force Inspector General, Office of the Secretary of the Air Force, and **provides a full range of CI services** encompassing four primary mission areas: collection, analysis and production, operations, and investigations. These missions are accomplished through proactive and reactive programs in support of Service, combatant command, and national-level agencies. AFOSI's primary responsibility during all levels of conflict is to provide Air Force commanders CI support to identify and neutralize the sabotage, clandestine intelligence, subversive, terrorist, and criminal threat to resources. In war or MOOTW, a realignment of AFOSI forces may be accomplished to meet the commander's requirements.

d. **US Marine Corps**

(1) **Director of Intelligence (DIRINT).** The DIRINT is the Commandant's principal intelligence staff officer and the functional manager for intelligence, counterintelligence, and cryptologic matters. Through the Intelligence Division, HQ Marine Corps, DIRINT allocates resources and manpower to develop and maintain specific expertise in the areas of human and technical reconnaissance and surveillance, GMI, HUMINT, CI, IMINT, SIGINT, and TENCAP.

(2) **US Marine Corps Intelligence Activity.** MCIA is a field activity under the DIRINT and the Marine Corps Service production center. MCIA is located at Quantico, Virginia with elements collocated with the Navy's NMIC at Suitland, Maryland. MCIA supports:

(a) The Commandant of the Marine Corps and his staff with threat assessments, estimates, and intelligence for Service planning and decision making.

(b) Combat developers with threat data and other intelligence support for doctrine and force structure development, systems and equipment acquisition, wargaming, and training and education.

(c) Operating force requirements for predeployment planning, training, and exercise, as well as support to contingency planning and other production not satisfied by either theater, other Service, or national research and analytic capabilities.

(3) As the production manager and validation authority for the Marine Corps production requirements, MCIA is fully integrated into the DODIPP. Through DODIPP, and the Joint Staff J-2 directed federated production program, MCIA can be tasked to provide expeditionary warfare intelligence to support any national, theater, or operational command in the Armed Forces of the United States. Thus, MCIA's unique and tailored analysis and production capabilities, to include its reserve production elements, supports not only the Marine Corps, but also national decision makers, combatant commanders, and operational forces.

ANNEX A TO APPENDIX B
JOINT CENTERS

1. Joint Information Operations Center

The JIOC, a subordinate element of USSTRATCOM, serves as the principal field agency within DOD for non-Service specific IO support. The primary mission of the JIOC is to provide direct IO support to operational commanders. Additionally, the JIOC will provide general support to OSD, the Joint Staff, the Services, US agencies, NATO, and allied nations. The JIOC integrates the constituent elements of IO — OPSEC, PSYOP, military deception, EW, and computer network operations — throughout the planning and execution phases of operations. The JIOC executes its mission through its directorates of Operations, Protection and Defense, and Technology Integration.

2. Joint Warfare Analysis Center

a. The JWAC, a USJFCOM subordinate element, is located at the Naval Surface Warfare Center in Dahlgren, Virginia. Like the JIOC, JWAC is not strictly an intelligence organization; however, a significant portion of its work supports intelligence applications.

b. The JWAC assists the Chairman of the Joint Chiefs of Staff and the combatant commanders in preparation and analysis of joint OPLANs and assists the Service Chiefs in the analysis of weapon effectiveness. JWAC serves as the Joint Staff agent for the integration and analysis of data concerning infrastructure networks. JWAC supports the combatant commands and the Joint Staff as prioritized by USJFCOM J-3. Secondarily, it provides support to the Military Services, OSD, and other government agencies as tasked by USJFCOM J-3.

c. The JWAC executes its mission through the following directorates: Intelligence; Operations; Information Systems; and Strategic and Technical Initiatives. Within these directorates, JWAC maintains a regional focus aligned with the geographic combatant commands.

Intentionally Blank

ANNEX B TO APPENDIX B
OTHER GOVERNMENTAL ORGANIZATIONS

1. Office of National Drug Control Policy

The Director of ONDCP is responsible for establishing policies, objectives, and priorities for the National Drug Control Program and for annually promulgating a National Drug Control Strategy to be submitted by the President to the Congress. The Director advises the President regarding necessary changes in the organization, management, budgeting, and personnel allocation of Federal agencies involved in drug enforcement activities.

2. The Drug Enforcement Administration, Department of Justice

The Drug Enforcement Administration (DEA) enforces laws and regulations governing narcotics and controlled substances, chemical diversion, and trafficking. It is also the lead agency overseas for counterdrug law enforcement activities and investigations. DEA makes ancillary contributions to the national IC via efforts to build legal cases against narcotics traffickers. DEA-collected and produced information is valuable in homeland security due to the traditional close association between narcotics trafficking and illegal alien smuggling. This results in DEA information potentially having significant value in counterterrorism applications.

3. Defense Threat Reduction Agency

DTRA's mission includes preventing the spread of WMD, responding to military requirements to help the United States deter, withstand, prevail against and recover from the use of such weapons, and preparing the combatant commands to counter the full spectrum of future WMD threats. DTRA's widespread inspection activities require close coordination with, and support from, IC members.

4. Counterintelligence Field Activity

CIFA is a field activity within the Department of Defense, under the authority, direction, and control of USD(I). CIFA's mission is to develop and manage CI programs and functions that support the protection of DOD personnel, resources, critical information, research and development programs, technology, critical infrastructure, economic security, and US interests, against foreign influence and manipulation, as well as to detect and neutralize espionage against DOD activities. CIFA is also responsible for overseeing DOD-wide CI investigations, operations, and CI functional services, to include oversight of CI investigations and operations in support of or arising out of joint operations.

5. Other USG Sources of Information

There are a number of "nonintelligence" USG agencies and organizations responsible for gathering and maintaining information and statistics related to foreign governments and international affairs. Such organizations as the Library of Congress, the Departments of Agriculture and Commerce, the National Technical Information Center, and the US Patent Office are potential sources of detailed, specialized information on political, economic, and military-related topics. The national-level IC may draw on these

organizations to support and enhance research and analysis and for relevant, peripheral data and background information for planners and decision makers.

ANNEX C TO APPENDIX B
INTELLIGENCE SYSTEMS IN SUPPORT OF CRISIS OPERATIONS

1. DIA

a. **NIST Fly-away Kits.** DIA/J-2O maintains an organic secure communications capability for support of crisis operations. This quick reaction capability is based on the International Maritime Satellite (INMARSAT) system and JDISS workstations and provides users with limited access to SCI and SIPRNET web pages, e-mail, joint collaborative intelligence tools, access to national intelligence databases, and one NSTS telephone line per kit. The deployable kits are capable of supporting three to five cleared individuals depending on the customer requirements. J-2O maintains a limited number of fully capable kits ready for immediate world-wide deployment in support of JCS directed operations.

b. **Containerized JWICS.** C-JWICS provides a portable JWICS communications capability to a deployed NIST or JTF. The C-JWICS is a deployable system in four transit cases that provides secure multimedia communications between the JTF and the IC. The C-JWICS gives the user access to the JWICS data network, JWICS VTC system, and to NSTS. The C-JWICS requires commercial power, a SCIF, and a communications path.

c. **JWICS Mobile Integrated Communications System.** The JMICS provides a JTF with a mobile JWICS communications system on a heavy, HMMWV and trailer. This mobile system provides secure Top Secret/SCI, high speed multimedia communications connectivity between the JTF and the IC. JMICS provides users with access to the JWICS data network, JWICS VTC system, the NSTS, secure telephone unit–III, and other communications feeds. JMICS is transported on a HMMWV, communications shelter, and a generator trailer. The system is transportable on C-130, C-141, C-17, and C-5 aircraft. It is typically deployed with a Trojan Spirit II communications transmission system although it can operate with commercial SATCOM systems. The JMICS is deployed at the direction of the Joint Staff J-2 in support of a combatant commander and/or JTF requirements.

2. NSA

a. **INMARSAT-B.** INMARSAT terminals can transmit either voice or data communications. INMARSAT provides expedient temporary access to JWICS during the initial stages of a deployment when no other pipeline is available.

b. **TRIBUTARY Fly-away package**: A TRIBUTARY fly-away package provides a portable, secure voice terminal using either military UHF, SATCOM media, or other LOS transmissions. It is designed for worldwide SATCOM or LOS communications access. Each unit is deployed as a self-contained case that provides all interconnect wiring, speaker system, antenna, and handset in a hinged equipment box for easy installation and repair. The NSA/SSA uses TRIBUTARY fly-away packages for worldwide threat warning broadcasts over the TRIBUTARY network. The TRIBUTARY network consists of a number of dedicated UHF secure SATCOM nets providing 24-hour secure voice communications support between national agencies and geographic combatant commands. TRIBUTARY

packages are also deployed with the "light" version of the CS communications suite (CS Lite) as a backup emergency communications system.

c. **Critical Source Lite**: CS Lite is a preconfigured communications suite containing a communications center and satellite equipment. The suite provides access/connectivity to the following systems: NSTS secure voice, National Security Agency Network, JWICS, and SIPRNET. The network connections will allow the analyst/customer access to the JWICS data network, the National Time-Sensitive System, and selected NSA databases authorized on a case-by-case basis. The customers are required to provide the appropriate hardware (computers, printers and servers etc.), software loads, user login and password for terminals and databases. The supported commander is responsible for the following: certified tactical sensitive compartmented information facility, power, environmental controlled operating area and billeting spaces.

3. CIA

The CIA element of the NIST deploys with its own secure satellite communications package. These communications provide direct connectivity between the JTF and CIA HQ and worldwide stations and bases. The fully redundant communications package is capable of secure voice and data transmissions as a stand-alone communications system, and can also interface with the JWICS and JMICS.

ANNEX D TO APPENDIX B
INTELLIGENCE RESOURCE PROGRAMS

1. Introduction

A large number of organizational elements have evolved in the intelligence arena to manage intelligence and intelligence-related activities. The numerous activities and assets that comprise the total US national intelligence effort fall within a broad spectrum ranging from strategic to tactical. There are three major intelligence groups that manage all intelligence activities and directly contribute to effective and coherent support to military intelligence consumers: NFIP, JMIP, and TIARA. The NFIP serves national-level decision makers across multiple government agencies and departments with primarily strategic intelligence. The JMIP provides intelligence to joint mission-oriented customers defense-wide. TIARA is focused on individual Military Services or agencies whose principal consumers are operational and tactical military commanders. Each of the three intelligence categories are addressed in this annex.

2. Resource Programs

a. Intelligence activities and assets are grouped and funded according to their function and/or purpose. Strategic intelligence typically is considered to be national-level activities and assets funded under a number of resource programs referred to collectively as the NFIP. Strategic or national intelligence primarily supports the President and national-level political and military leadership. It is primarily strategic in nature, concerns plans and intentions of foreign entities, and serves as the basis for the national military strategy. The NFIP is jointly managed by the Deputy Secretary of Defense and the DCI. The NFIP resources provide the funding for intelligence activities and assets necessary for intelligence operations to support the US military for EAC. It is conducted by a wide range of intelligence organizations (see top arrow Figure B-D-1).

b. The JMIP was established to improve the effectiveness of DOD intelligence activities when those activities involve resources from more than one DOD component; when the users of the intelligence data are from more than one DOD component; and/or when centralized planning, management, coordination, or oversight will contribute to the effectiveness of the effort. The JMIP focuses on joint, defense-wide initiatives, activities, and programs that provide more effective and coherent intelligence programmatic decision making (see middle arrow Figure B-D-1). Military intelligence consumers supported include the warfighter, policymaker, and force modernization planners. JMIP-funded activities are managed by the Deputy Secretary of Defense. JMIP and TIARA constitute the basis for Defense intelligence outside the NFIP.

c. TIARA resources provide the funding of tactical intelligence, related activities, and assets necessary for military operations at the corps, wing, naval battle group, and Marine expeditionary force level and below (see bottom arrow Figure B-D-1). TIARA-funded activities are managed under the direction of the Secretary of Defense. The programs are designed, built, and operated by the Military Services and Defense agencies and compete for funding with combat and combat-support programs. TIARA funds represent those portions of the DOD budget devoted to non-NFIP intelligence and other related activities that respond to combatant commander's

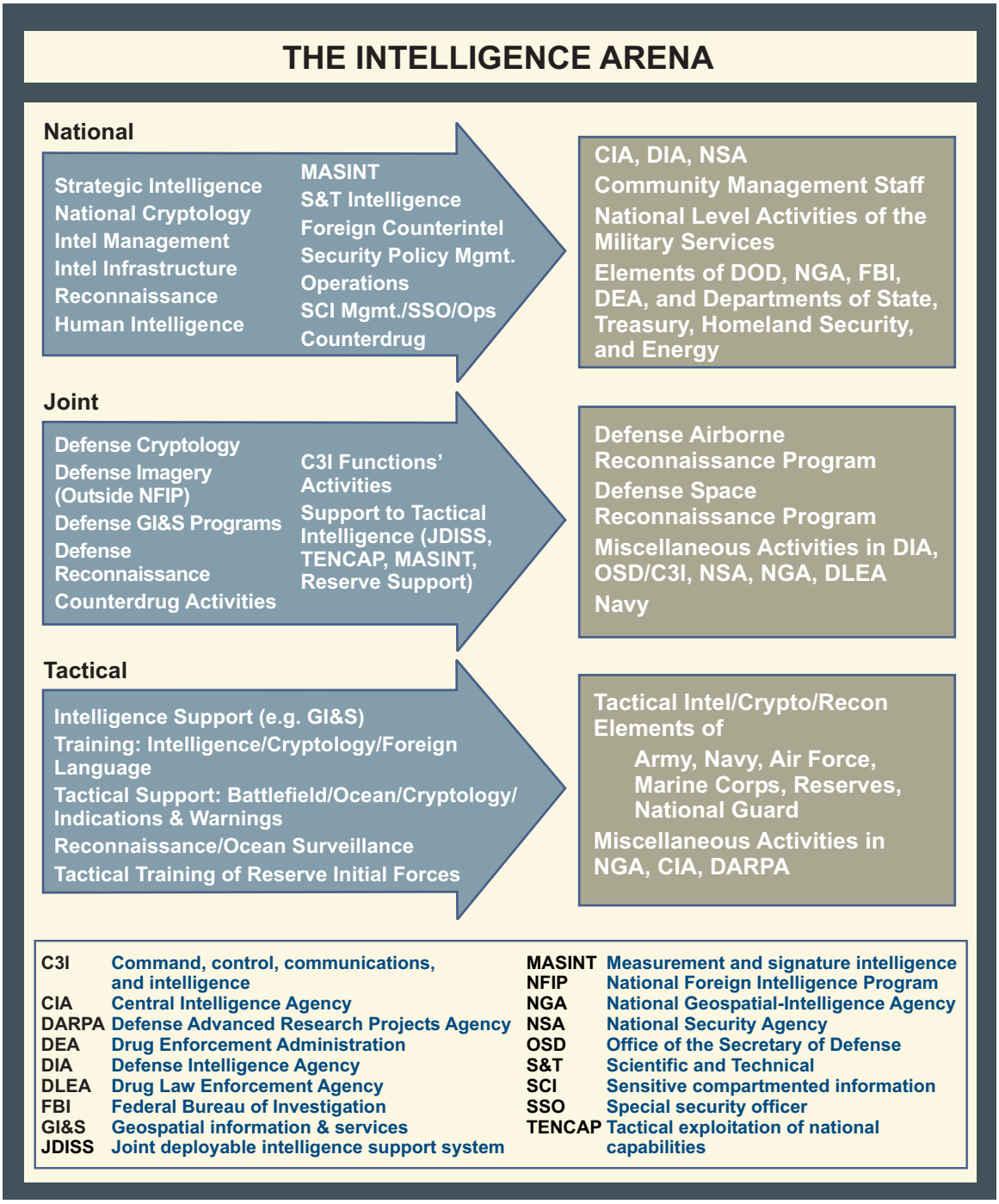


Figure B-D-1. The Intelligence Arena

requirements to gather and interpret time-sensitive intelligence on foreign entities. TIARA includes programs that fund intelligence training, reserve forces, and research and development. A universal "rule of thumb" is anything that is not NFIP or JMIP-funded must be considered either a tactical-level intelligence asset (i.e., TIARA) or something other than an intelligence asset (i.e., operational).

3. National Foreign Intelligence Program

a. The NFIP provides funds for the bulk of national-level intelligence, foreign CI, and reconnaissance activities of the IC as well as other USG intelligence programs designated for inclusion in the NFIP by the heads of the executive department involved and the DCI or the President.

b. Each NFIP program is headed by a program manager who prepares the program's annual budget and oversees the expenditure of the funds allocated to the program. While some NFIP programs are managed by the heads of organizations most closely associated with them (e.g., the Consolidated Cryptologic Program [CCP] by the Director of NSA), others are not (e.g., the Central Intelligence Agency Program [CIAP] is not managed by the DCI, but by the Deputy Director of CIA). The program managers receive policy and fiscal guidance from the DCI and prepare and submit their programs' budget for DCI approval and consolidation into the single NFIP budget which is submitted to the President.

c. The NFIP budget is not openly published for national security reasons. NFIP funding is actually embedded within elements of the Defense budget. These funds are administered by the Military Services, but under the close scrutiny of NFIP program managers.

4. General Defense Intelligence Program

a. The broadest-based NFIP program within the Department of Defense and Military Services is the GDIP. This program funds MI units and activities that involve functions other than cryptology, CI, and certain types of specialized reconnaissance. It includes DIA, intelligence units from each of the Military Departments, and combatant command units that have theater-wide responsibilities and significant national or departmental intelligence missions.

b. The GDIP encompasses the following activities.

(1) All defense intelligence production not funded elsewhere in the NFIP.

(2) All national-level DOD human source intelligence.

(3) A wide range of activities that provide defense intelligence infrastructure.

(4) Significant collection (other than cryptologic and CI) against geographic targets, foreign forces, and foreign weapon systems.

c. GDIP-funded units and activities collect information, process and analyze data, and produce MI for the following spectrum of missions:

(1) **Support to warfighting**

(a) Input to national military strategy.

(b) I&W.

(c) Countermeasures and military contingency operations.

(d) Theater-level battle planning and direction of combat operations.

(e) Planning and conducting small scale contingency operations (e.g., noncombatant evacuation operations).

(2) **Equipping and training of forces**

(a) Weapons and countermeasures acquisition.

(b) Force structure development.

(c) Doctrine and tactics training.

(d) Military education and training.

(3) **Direct support for national-level priorities**

(a) Foreign policy development.

(b) Arms control negotiations and treaty monitoring.

d. Units and activities funded by the GDIP must be tasked to perform their principal intelligence mission and must support missions of the Department of Defense, a Military Department, a combatant command, or more than one component command.

(1) The GDIP supports OSD and JCS decision making; Military Service training and equipping; and production, collection, information systems, or intelligence communications capabilities within combatant commands, JICs, and component HQ.

(2) GDIP is affected by resource decisions and actions of other programs within the NFIP and TIARA. For example, GDIP often funds the training of operators of new systems acquired through other programs. It also provides equipment and communications for other systems to ensure interoperability and compatibility with other systems funded outside the GDIP.

e. GDIP funds are expended mainly in the four following areas of intelligence:

(1) **Production**

(a) GDIP-funded production includes all Defense intelligence production in the NFIP (except SIGINT, MASINT, and CI) and supports the timely production of fused all-source finished intelligence for warfighters and the national, Service, and departmental leadership. Its

products include databases of foreign military forces and programs, targeting materials, scientific and technical (S&T) analyses, and threat assessment.

(b) The Director, DIA is the Program Manager of the GDIP and the agency is one of the major producers. DIA produces a full range of basic, current, warning, and estimative intelligence that supports geographic combatant commanders and operational forces, the Military Departments, and national policymakers.

(c) Military Service producers focus mainly on national-level intelligence needed to equip and train forces to support the combatant commanders and maintain S&T centers and operational intelligence centers funded through the GDIP.

(d) A significant portion of GDIP intelligence production is accomplished in theater intelligence production centers, imagery centers, and component analytical centers.

(2) **Collection.** The GDIP funds intelligence collection primarily in three areas.

(a) HUMINT.

(b) MASINT conducted through a variety of systems ranging from national technical means to ground-based systems.

(c) Collection (other than SIGINT and certain other types of collection conducted through other NFIP programs) against geographic targets and foreign forces and weapon systems. The collection is achieved mainly through technical sensors on airborne reconnaissance platforms and aboard a variety of other collection systems.

(3) **Infrastructure.** This third aspect of the GDIP includes the following:

(a) **Automation.** DODIIS intelligence systems support and automated intelligence systems, as well as noncryptologic communications for SCI dissemination.

(b) Reproduction, presentation, and dissemination of a wide range of intelligence materials and data.

(c) Physical, personnel, industrial, computer, telecommunications, and operations security. This includes noncryptologic SCI policy and operations as well as adjudication of special background investigations.

(d) Intelligence training and education, such as the courses conducted at the Joint Military Intelligence College.

(4) **Management.** GDIP funds three types of intelligence management: program intelligence management, functional management, and fiscal management. Program management was discussed earlier in this annex. Functional managers and their staffs are oriented along the

three broad functional areas of production, collection, and infrastructure which encompass the full range of activities funded under the GDIP. Fiscal management involves the GDIP programming and budget process, a structured sequence within the NFIP that runs parallel to that of all other NFIP programs against which GDIP requests eventually compete for a share of the NFIP budget. The process begins when the GDIP Program Manager receives guidance from the DCI and uses it to develop his own "top-down" policy and fiscal guidance, in the Program Manager's Guidance Memorandum (PMGM), to the Service intelligence elements, DIA, and the combatant commands. Based on the Program Manager's guidance, the functional managers provide funding priorities and specific guidance relative to their respective area of concern which is included in the PMGM.

5. Other NFIP Programs

a. **Central Intelligence Agency Program.** The activities of CIA are funded under the CIAP. This NFIP program provides funds for analytical and controlled activities, administration, field operations, and research and development. The Deputy Director of the CIA is designated as the Program Manager of the CIAP.

b. **National Geospatial-Intelligence Agency Program (NGP).** The NGP funds all NGA national level programs. The Director, NGA is designated as the functional manager of the NGP.

c. **Consolidated Cryptologic Program.** CCP is operated and managed by NSA, with the DIRNSA serving as the Program Manager. In addition to its own worldwide SIGINT and OPSEC operations, NSA also oversees national-level operations of the three Service cryptologic elements. These elements include the Naval Security Group, the cryptologic components of the Army's INSCOM, and the Air Intelligence Agency.

d. **DOD Foreign Counterintelligence Program.** This component of the NFIP conducts CI activities in support of DOD components OCONUS in coordination with the CIA, and within the US in coordination with the FBI, pursuant to procedures agreed upon by the Attorney General and the Secretary of Defense.

e. **Special Reconnaissance Intelligence Programs in DOD.** Two sensitive programs collect specialized intelligence through reconnaissance. These programs are responsible for:

(1) Carrying out consolidated reconnaissance programs for specialized intelligence.

(2) Responding to taskings IAW procedures established by the DCI.

(3) Delegating authority to the various agencies and departments for research, development, procurement, and operation of designated means of collection.

f. **Treasury Department Intelligence Program.** This NFIP program is that element of the Treasury responsible for:

(1) Overt collection of foreign financial and monetary information.

(2) Participation with the DOS in the overt collection of general foreign economic information.

(3) Production and dissemination of foreign intelligence relating to US economic policy as required for the execution of the responsibilities of the Secretary of the Treasury.

g. **State Department Bureau of Intelligence and Research.** This NFIP organization is that element of the State Department that:

(1) Overtly collects information relevant to US foreign policy concerns.

(2) Produces and disseminates foreign intelligence relating to US foreign policy as required for the execution of the Secretary of State's responsibilities.

(3) Disseminates, as appropriate, reports received from US diplomatic and consular posts.

(4) Transmits reporting requirements of the IC to the chiefs of US missions abroad.

(5) Supports chiefs of missions in discharging their statutory responsibilities for direction and coordination of mission activities.

h. **FBI Foreign Counterintelligence and International Terrorism Program.** This NFIP element is responsible for:

(1) Conducting CI activities within the United States.

(2) Conducting CI activities OCONUS in coordination with the CIA, as required by agreement of the DCI and the Attorney General.

(3) Collecting, producing, and disseminating foreign intelligence and CI.

(4) Carrying out research, development, and procurement of technical systems and devices related to their authorized functions.

i. **Department of Energy Intelligence and Satellite Instrumentation Program.** This program is responsible for:

(1) Participating with the DOS in overtly collecting information with respect to foreign energy matters.

(2) Participating in formulating intelligence collection and analysis requirements where the special expert capability of the DOS can contribute.

(3) Providing expert technical, analytical, and research capability to other agencies within the IC.

j. **Special NFIP Accounts.** In addition to the programs described above, there are two additional accounts managed as part of the NFIP. These two accounts are the CIA Retirement and Disability System and the Security Evaluation Program.

6. Joint Military Intelligence Program

a. The JMIP is designed specifically to improve the oversight of selected Defense-wide intelligence programs and resources. Defense-wide resources are those initiatives, activities, and programs that predominantly provide intelligence information and support to multiple Defense consumers. The JMIP institutes a management system to oversee programs intended for multiple users, and/or cross-Service support, to ensure genuine responsiveness to the requirements of those who are to be supported and to revitalize the concepts of commonality and interoperability.

b. As the Program Executive, the Deputy Secretary of Defense provides policy and substantive programmatic and fiscal guidance for the JMIP and exercises review and approval authority over JMIP and any subsequent program modifications that significantly alter cost, schedule, or capability. Reprogramming of JMIP funds requires the approval of the Program Executive.

c. The JMIP is composed of three major programs:

(1) **Defense Cryptologic Program.** The Program Manager is DIRNSA.

(2) **Defense Imagery and Mapping Program.** The Defense Imagery and Mapping Program funds defense-wide GI&S activities, including production, communications, and production system improvements as well as the defense imagery activities of NGA. Also funded are selected defense airborne and space reconnaissance activities managed by NGA. The Program Manager is the Director, NGA.

(3) **Defense General Intelligence and Applications Program.** The Program Coordinator is the Director, DIA.

d. The DGIAP is comprised of five component programs. Each program focuses on a certain key area of joint support. The Program Coordinator works with each component to best integrate and utilize available resources and assists the five DGIAP component managers in developing their program submissions, resolving programmatic issues across the DGIAP and, in conjunction with those program managers, resolves issues across the JMIP. As such, the DGIAP Program Coordinator is the principal interface with the other JMIP programs, NFIP, and TIARA.

(1) The component programs include:

(a) Defense Airborne Reconnaissance Program.

(b) Defense Intelligence Tactical Program.

(c) Defense Intelligence Counterdrug Program.

(d) Defense Intelligence Special Technologies Program.

(e) Defense Space Reconnaissance Program.

(2) Each of the above programs consists of former TIARA or selected NFIP programs whose primary customer base was judged to be multiple Service and defense-wide.

e. The JMIP uses the DOD Planning, Programming, and Budgeting System. The JMIP management process avoids the establishment of dedicated panels or working groups to raise and resolve issues by employing existing boards such as the Intelligence Systems Board, the MIB, and the Military Communications and Electronic Board.

Intentionally Blank

APPENDIX C
REPRESENTATIVE INTELLIGENCE REQUIREMENTS

1. Overview

An illustrative table of intelligence requirements is provided as a starting point for developing a mission specific list. This reflects the probable intelligence needs of a combatant commander. The list is representative of the major concerns of a commander at any level, but is not offered as a definitive, exhaustive compilation of every possible concern. A combatant command J-2 or subordinate joint force J-2 preparing PIRs for the commander's approval can use this table to stimulate ideas and to identify information gaps, especially since different Service and/or functional components may require more detailed information than outlined in the intelligence requirements provided below. The mission-specific list should be prioritized to ensure that collection decisions can be made rationally and that the intelligence effort remains focused on responding to the most important requirements first.

2. Intelligence Requirements

a. **Assess Damage**

(1) Assess Damage 1. Assess target audience behavior change and determine mission success as defined by PSYOP objectives and measures of effectiveness.

(2) Assess Damage 2. Assess extent of soft or hard damage to adversary combat units in order to plan restrike and follow-on phases of the operation.

(3) Assess Damage 3. Assess status and adversary ability to repair, reconstitute, recuperate, or relocate vital infrastructure, weapon systems and forces. Provide data which allows assessment of mission results against overall campaign objectives and tactics.

(4) Assess Damage 4. Determine the level of casualties at which the specific adversary considers his units to be combat ineffective and identify which military units have sustained at least that level of casualties.

(5) Assess Damage 5. Assess the extent, type, and operational implications of attack on a WMD facility.

b. **Beach Defenses.** Determine adversary beach defenses; provide timely surveillance; locate and/or identify coastal defense units (priority on artillery, mechanized infantry, and armored units).

c. **Casualties.** Predict number of friendly and adversary casualties and chemical, biological, or radiation injuries to estimate transportation, hospital space and medical support required.

d. **Commercial Traffic**

(1) Commercial Traffic 1. Identify air, sea and ground commercial routing, traffic, and density within the operational area. Identify commercial air corridors.

(2) Commercial Traffic 2. Provide information on all shipping to include suspected carriers of contraband, major ports of debarkation, historic shipping density data, and daily operation summary of expected departures, arrivals, and schedules. Identify types of vessels.

e. **Counterintelligence.** Describe adversary's awareness or knowledge of, and countermeasures to, US intelligence activities.

f. **Personnel Recovery**

(1) Personnel Recovery 1. Assess adversary capabilities to threaten recovery forces, including rotary-wing aircraft. Include disposition, strength, capabilities, and activities of air, ground, maritime, special operations, paramilitary, and security forces.

(2) Personnel Recovery 2. Describe adversary electronic capabilities to detect, locate, track, jam, or deceive recovery forces.

(3) Personnel Recovery 3. Identify adversary resources used to find isolated personnel (direction finding equipment, helicopters, dogs, infrared trackers, night vision goggles, etc.).

(4) Personnel Recovery 4. Analyze the policy, practices, and intentions of adversary or neutral countries toward friendly isolated personnel, hostages, detainees, prisoners of war, and recovery forces.

(5) Personnel Recovery 5. Estimate the attitude of the populace toward isolated personnel, including their susceptibility to adversary pressure to provide information about or assist in the search for isolated personnel. Include information about minority or opposition groups that may assist, or at least not oppose, evasion and personnel recovery operations.

(6) Personnel Recovery 6. Collect and analyze information about the physical environment pertinent to isolated personnel and recovery forces to include terrain, climate and weather, food and water sources, flora and fauna, concealment, LOCs, and avenues of approach.

(7) Personnel Recovery 7. Locate and characterize potential detention or interrogation facilities and medical facilities where personnel may be held

g. **Computer Network**

(1) Computer Network 1. Describe the key components of an adversary's computer network infrastructure.

(2) Computer Network 2. Identify key components and potential vulnerabilities of friendly computer networks.

(3) Computer Network 3. Evaluate adversary's ability to conduct or direct network attack activities.

h. **Demographics/Culture**

(1) Demographics/Culture 1. Identify languages, dialects, ethnic and tribal composition (both national and target area).

(2) Demographics/Culture 2. Describe customs (social, weapons, religious, cultural, mores).

(3) Demographics/Culture 3. Identify tensions (regional and national; causes, intensity, degree, and exploitability by the United States or opposition).

(4) Demographics/Culture 4. Identify foreign influences (sources, leaders, themes, influence on government, unions, students, insurgents and general public).

(5) Demographics/Culture 5. Characterize attitude of civilians and civilian groups to US involvement (friendly, unfriendly, or neutral), and for planned US operations (support, oppose, tolerate).

(6) Demographics/Culture 6. Estimate assistance available to US forces (extent and capabilities, laborers, linguists, liaison, analysts, administrators); determine attitude of neutral population toward host country, threat policies, and actions.

(7) Demographics/Culture 7. Determine probable reactions of leadership and population in country to US UW or other SOF activities. Determine how a country (government and population) will treat those indigenous personnel who participated in wartime UW or SOF activities in a post-conflict environment.

i. **Demographics/Economics**

(1) Demographics/Economics 1. Assess civilian economy and war sustaining infrastructure; include community structures, industrial base and complexes, resources and strategic reserves, petroleum production, storage and/or distribution, weapons systems and/or munitions, research and development, stockpiles, electric power, and transportation.

(2) Demographics/Economics 2. Estimate available labor force (location, numbers, equipment, skills).

(3) Demographics/Economics 3. Assess effect of any UN and/or international sanctions on the country's ability to wage war.

(4) Demographics/Economics 4. Identify civilian supply shortages. List commodities available for potential use by US forces. Determine status of local food or market distribution system. Identify food stocks, stockpiles, and warehouses.

(5) Demographics/Economics 5. Identify the location, type, and quantity of TIM for potential impact on operations or consequences if the facility is attacked.

j. **Demographics/Information**

(1) Demographics/Information 1. Describe information or propaganda service, apparatus, or organization (key personnel, attitude toward the USG, whether usable by US forces) and employment of propaganda and disinformation (current, future capabilities).

(2) Demographics/Information 2. Determine if military personnel have access to commercial radios and/or televisions; automated information management systems; type of printed material they carry, literacy rate, languages used. Provide samples.

k. **Demographics/International**

(1) Demographics/International 1. Describe country's diplomatic activity.

(2) Demographics/International 2. List membership in international organizations (UN) or groups (Red Cross).

(3) Demographics/International 3. Characterize human rights history (friendly and threat countries) and US policy toward country's human rights actions.

(4) Demographics/International 4. Describe country's government or popular support of regional insurgencies (groups, movements, type of support).

(5) Demographics/International 5. Identify foreign military or political agents of influence within country.

l. **Demographics/Medical**

(1) Demographics/Medical 1. Determine the health threat to friendly forces. Describe local diseases, extreme environmental conditions, locally available illegal drugs, and flora and fauna which may contribute to the health threat.

(2) Demographics/Medical 2. Determine local public health facilities status and needs, to include level of staffing available; specific health services provided; health and sanitation conditions; major health-related problems; shortages of medicines, pharmaceuticals, or equipment including transportation.

m. **Demographics/Miscellaneous.** Miscellaneous (including currency, holidays, dress, customs, and foreign influences).

n. **Demographics/Political**

(1) Demographics/Political 1. Opposition to existing US forces, facilities, or interests (general population and significant groups and forces).

(2) Demographics/Political 2. Describe adversary nation's political leadership structure and dynamics, with particular emphasis on C2 facilities. Describe country's political structures, parties, and leadership organizations.

(3) Demographics/Political 3. Describe country's internal groups (indigenous elements who are members, level of popular support, group's support or nonsupport of governing regime).

(4) Demographics/Political 4. Provide biographical sketches of all significant political leaders and advisors and military leaders down to division level (background, education, talents, connections, political affiliations, orientation, US training).

(5) Demographics/Political 5. Describe anti-government opposition groups or resistance forces (names, organization, leaders, political affiliation, size, support), military capabilities (organization, equipment, training, ability to conduct sabotage, subversion, deception), and communications.

(6) Demographics/Political 6. Determine threat to US personnel from opposition or resistance groups.

(7) Demographics/Political 7. Identify military or civilian leaders within potential insurgent groups who will support coalition efforts.

(8) Demographics/Political 8. Identify military or civilian leaders within potential insurgent groups who would make acceptable post-hostility leaders. Identify military and civilian leaders, whom, if protected, would enhance post-hostility restructuring.

(9) Demographics/Political 9. Assess vulnerabilities of objective country government to insurgent attack (prioritize).

(10) Demographics/Political 10. Identify US-provided materials or services urgently needed or required by cooperating indigenous military, paramilitary, resistance forces, or local nationals.

o. **Demographics/Population.** Describe area population characteristics.

p. **Demographics/Refugees.** Estimate number of dislocated civilians, disruption to civilian infrastructure, and refugee movement. Identify and locate camps and camp managers. Determine support requirements (shortages of food, medicine, shelter, clothing).

q. **Demographics/Religion.** Describe key religions and impact on ethical or decision-making processes. Identify key religious leaders, factions, and groups.

r. **Demographics/Social Conditions**

(1) Demographics/Social Conditions 1. Describe civil disturbance and riot control training (units and their capabilities).

(2) Demographics/Social Conditions 2. Determine status and needs of local public administration and law enforcement. Can local, regional, or national administrators continue essential functions? Identify key leaders of the various civil agencies or departments. Status of jails and prisons.

(3) Demographics/Social Conditions 3. Determine status and capability of power, telecommunications, water, sewage, refuse collection, fire-fighting, and public transportation services. Are facilities secured (by whom)? Identify capability to transport water (trailer, tanker). Is local water potable?

s. **Environment.** Describe adversary intentions and capabilities to conduct environmental warfare (oil dumping, ignition of oil field fires, release of toxins).

t. **Geography**

(1) Geography 1. Characterize objective area, including country(s), geographic limits of objective area (geographic or universal transverse mercator coordinates), and plan or operation (number and name).

(2) Geography 2. Describe and state the significance of objective area.

(3) Geography 3. Describe geographic terrain features (general description, key natural and manmade features).

(4) Geography 4. Describe flora and fauna. Include information of tactical value, e.g., plants and animals that would impede or assist movement routes, rates, massing, dispersal, identification and acquisition of forces; the effects on weapon capabilities; and security considerations.

(5) Geography/Approaches. Avenues of approach into objective area (road, rail, waterway, air) with most likely approach of reinforcements; obstacles, choke points, terrain features; special conditions (seasonal variations); fording sites (depth, width, type bottom); trafficability (transit).

(6) Geography/Hydrography 1. Provide hydrographic data (coastal, waterways, lakes), to include tidal activity; currents; temperatures; special conditions (seasonal variations); and depths and underwater obstacles.

(7) Geography/Hydrography 2. Identify water sources (type, source, location, capacity).

(8) Geography/Hydrography 3. Provide detailed terrain and/or hydrographic data on landing beaches within the objective area to include nearshore and/or offshore bathymetric data (currents, tides, wave height, depth, reef conditions, location of sandbars, beach gradients, frontage, composition, obstacles).

(9) Geography/Geospatial Information and Services 1. Provide terrain data (i.e., prominent geographical or manmade structures that could be used as navigational aids for aircraft, troops, cruise missiles or precision-guided munitions [PGMs]; and characteristics of slope, soil analysis, or surface material) to determine trafficability.

(10) Geography/Geospatial Information and Services 2. Provide terrain maps, charts, overlays, imagery, or pictomaps in both printed and digital form.

(11) Geography/Geospatial Information and Services 3. Provide ocean charts for deploying naval forces.

(12) Geography/Meteorology and Oceanography 1. Describe METOC conditions to support air, ground, and naval operations, artillery, surface-to-surface missile, cruise missile, PGMs, reconnaissance, surveillance, and communications operations.

(13) Geography/Meteorology and Oceanography 2. Provide historical METOC data (including unusual conditions such as sandstorms, blizzards).

u. **Geopolitical**

(1) Geopolitical/Allies and Coalition Partners. Assess true capabilities and vulnerabilities of non-US multinational forces.

(2) Geopolitical/Intentions. Determine country's strategic intentions. Identify country's criteria for success.

(3) Geopolitical/Reaction 1. Determine the reaction of potentially hostile, allied, or neutral international, political, civilian, military, and paramilitary elements to insertion of US forces into the AOR and/or JOA before or after initiation of hostilities. Will a third party intervene?

(4) Geopolitical/Reaction 2. Identify neighboring countries or non-state actors that have taken any measures or may attempt to disrupt US air mobility and/or sealift operations. Describe their capabilities, e.g., units, tactics. Determine which resources will be used.

(5) Geopolitical/Reaction 3. Identify countries en route to or in the AOR and/or JOA which will or may deny US overflight, landing rights, or docking privileges.

(6) Geopolitical/Reaction 4. Determine which potential hostile and/or target countries in the AOR and/or JOA have detected US preparations to conduct or support military operations in the AOR and/or JOA. Estimate their reaction.

v. **Host-Nation Support**

(1) HNS. Describe logistic infrastructure existent within the coalition area for use by US and/or coalition forces. Estimate level of HNS that US forces can expect. Identify and determine the severity of threats to HNS efforts.

(2) HNS/Logistics. Identify suitable beaches and/or terrain available for joint logistics over-the-shore operations.

(3) HNS/Ports 1. Describe sea ports (port infrastructure, operational considerations, fuel, cargo handling, transshipment, security).

(4) HNS/Ports 2. Describe airports (type, status, activity), defenses (friendly and unfriendly), combat operations, facilities, infrastructure, support facilities.

(5) HNS/Transportation 1. Describe transshipment or transportation capability from air and sea ports. Identify major obstacles, choke points, limitations, and alternative routes.

(6) HNS/Transportation 2. Identify critical C4 and transportation nodes which, if destroyed, would have an adverse impact on USTRANSCOM's ability to deploy and sustain US combat forces.

w. **I&W**

(1) I&W 1. Provide I&W of potential hostile attacks such as movement of aircraft to dispersal bases; unusual out of garrison deployments; distribution of wartime stores and supplies; changes in readiness, alert, and mobilization postures.

(2) I&W 2. I&W indicators of preparation by the objective country or opposition forces for action within a 24-hour period for the following: attack, withdraw without engaging, reinforce, defend, delay, conduct special or WMD operations.

x. **Infiltration.** Identify and describe potential landing zones and drop zones, navigation landmarks and characteristics; availability to US forces; limitations on operations; choke points between insertion points and objective; and adversary forces threat information at zone and along route.

y. **IO.** Identify and describe adversary's offensive and defensive IO capabilities.

z. **Intelligence/Adversary Capability.** Identify, locate, and describe adversary intelligence and CI capabilities by type (SIGINT, HUMINT, IMINT), with particular emphasis on key facilities, surveillance measures, and night vision capabilities; include agency, means, effectiveness, biases.

aa. **LOCs**

(1) LOCs 1. Describe railways, to include status, description of network (graph, overlay, chart), and factors limiting use. List bridges, tunnels, ferries, locomotives, rolling stock, signal and control systems, railway gauge, terminals, rail transfer points.

(2) LOCs 2. Describe roadways to include status, description of network (graph, overlay, chart), factors limiting use, and bypass routes. List bridges, tunnels, ferries, fords, highway maintenance, vehicle types.

(3) LOCs 3. Describe waterways (graph, overlay, chart); beaches suitable for amphibious landing (beach length, configuration, usable length); interruptions and obstacles; type of coastline; backshore, foreshore, and nearshore description (width, gradient, composition).

(4) LOCs 4. List primary and exploitable modes of transportation (trucks, buses, river craft — government, public, and commercial).

(5) LOCs 5. Describe petroleum, oils, and lubricants (POL) (sources, reserves, natural gas stream, production, refining, storage, pipelines, pump and compressor stations, controls, storage tank farms, shipping terminals, distribution), to include development company and/or nation, vulnerabilities, and exploitability by US forces.

(6) LOCs 6. Describe power grid (generating and distribution networks, facilities, loads, maintenance, transmission lines, sources of energy, controls, blackout history, government organizations associated, development company and/or nation) to include vulnerabilities and exploitability by US forces.

(7) LOCs/Airfields. Describe airfields (graph, overlay, chart — type, location, capacity, POL, parking areas, aircraft, base operations and facilities, development company and/or nation) and factors limiting use and/or availability.

(8) LOCs/Information 1. Describe public information media and telecommunications to include status, controlling authority, signal allocation; radio and television broadcasts; print and newspapers; communications network, technologies, equipment, and operations.

(9) LOCs/Information 2. Determine status of civil telecommunications systems; identify existing links. Are sufficiently trained personnel available to fully man and operate the systems? Identify specific skill shortages. Are facilities secured (by whom)?

(10) LOCs/Seaports. Describe the threat country's seaports (port infrastructure, operational considerations, fuel, cargo handling, transshipment, security, development company and/or nation).

Identify vulnerabilities, port operation, commercial and military shipping traffic.

bb. **Military Assistance**

(1) Military Assistance 1. Identify countries committed to providing military assistance (legal, de facto); military advisors, and other personnel already present (noncombatants, medical, engineers, by country, location, type of assistance); combatants or paramilitary (strengths, locations).

(2) Military Assistance 2. Identify foreign technologies (communications, computers, software) or contractor services, and construction (type of work, frequency, purpose, equipment, location, country or company); and foreign nonweapons military materiel (trucks, heavy equipment).

(3) Military Assistance 3. Identify foreign or US materiel and services required by the threat nation. Can the country operate systems, forces, industries without foreign personnel, equipment, or supplies? How long? What is the impact of cutoff of foreign support? Status of LOCs.

cc. **Military Capabilities**

(1) Military Capabilities/Air Defense 1. Assess the capabilities and readiness, doctrine, tactics, vulnerabilities, intentions, location, disposition, and sustainability of air defense forces (surface-to-air missile [SAM], anti-aircraft artillery [AAA], radar, sensors) and their support facilities.

(2) Military Capabilities/Air Defense 2. Identify countries in AOR and/or JOA which show indications of preparing air defense forces to intercept US and/or allied air operations. Describe the long-range fighter intercept capabilities of the potential threat air defense forces (adversary and neighboring countries).

(3) Military Capabilities/Air Defense 3. Locate and identify capability to support ground forces with combat air and air defense resources (en route to and within the objective area), particularly at or around the forward edge of the battle area.

(4) Military Capabilities/Air Defense 4. Detect, locate, and identify SAM and AAA threat emitters and associated weapons along ingress and egress routes and within the objective area; determine operational status, readiness, and duty cycle of air defense radars within objective area of influence.

(5) Military Capabilities/Air Defense 5. Detect SAM launch.

(6) Military Capabilities/Air Defense, EW, and/or ground control intercept (GCI) Radars. Determine precise location and status of EW and/or GCI radar sites.

(7) Military Capabilities/Air Operations 1. Assess the capabilities, readiness, sortie rates, munitions, doctrine, tactics, vulnerabilities, intentions, location, disposition (count, track, identify, classify), and sustainability of threat air forces.

(8) Military Capabilities/Air Operations 2. Detect, identify by type, and locate threat aircraft launch event in operational area and determine type of onboard munitions.

(9) Military Capabilities/Air Operations 3. Track inflight threat aircraft within the operational area.

(10) Military Capabilities/Antimissile Defense/Adversary 1. Detect and identify any antimissile defense systems, especially those that could affect cruise missiles along flight path. Determine operational status of each such system.

(11) Military Capabilities/Antimissile Defense/Adversary 2. Detect, identify by type, and locate antimissile launch event.

(12) Military Capabilities/C4I 1. Detect, locate, classify, characterize and identify command posts and/or bunkers by type unit, computers, communications architecture, and critical C4I nodes.

(13) Military Capabilities/C4I 2. Describe country communications profile (type of information on circuit, type of communications, communications table of organization and equipment, pattern of employment, COMSEC equipment and methods, location), including computer connectivity.

(14) Military Capabilities/C4I 3. Detect wartime reserve mode usage and anticipated countermeasures.

(15) Military Capabilities/C4I 4. Determine adversary vulnerability to C2W; list communications of military significance including computers and susceptibility to C2W actions.

(16) Military Capabilities/C4I 5. Assess adversary C2W C2-attack and C2-protect capabilities and indications of employment.

(17) Military Capabilities/D&D 1. Detect, identify, locate, and characterize adversary D&D techniques with emphasis on use of decoys.

(18) Military Capabilities/D&D 2. Determine the deception techniques the adversary will most likely accept as truth. Assess the adversary's ability to detect and penetrate US D&D plan.

(19) Military Capabilities/Electronic OB. Assess the adversary's electronic resources (including country high value airborne resources, EW, GCI, fire control, tracking, and acquisition radars) capabilities. Evaluate resource location and disposition, sustainability, and vulnerabilities.

(20) Military Capabilities/EW. Assess capability to perform EW, C2W, suppression of enemy air defenses, beaconing, interference, jamming and intrusion, and electronic protection to include location, platform, type, specifications, and parametrics of equipment.

(21) Military Capabilities/Ground OB 1. Determine strength, status, location and identification of adversary forces with particular emphasis on armor, mechanized infantry, artillery, air defense, infantry, theater missile, WMD warfare units and munitions.

(22) Military Capabilities/Ground OB 2. Identify, describe and locate front-line adversary troop movements.

(23) Military Capabilities/Ground OB 3. Detect, locate, and classify possible assembly, staging, dispersal, repair and resupply areas with emphasis on mechanized and armored vehicles.

(24) Military Capabilities/Ground OB 4. Detect, locate, classify, identify, and determine composition of hostile forces capable of reinforcing the area and identify likely reinforcement routes. Identify, locate, and describe adversary follow-on forces and resupply capability.

(25) Military Capabilities/Ground OB 5. Detect, locate, and identify by type anti-armor and antipersonnel mines, ditches, barriers, antitank traps, obstacles, field defensive positions, and night vision capabilities along potential assault routes and within vicinity of objective area.

(26) Military Capabilities/Logistics 1. Locate and identify combat service and support units, to include: transportation units; forward logistic bases; repair and repair facilities; ammunition supply points and storage areas; and POL sites.

(27) Military Capabilities/Logistics 2. Identify military units which are experiencing equipment or logistic problems and identify the causes. Assess how these problems are affecting the unit mission.

(28) Military Capabilities/Naval 1. Identify, describe, detect and locate threat naval forces (including coast guard and maritime border guard) to include type, number, capability, equipment, weapons, readiness, doctrine, tactics, munitions, vulnerabilities, disposition, and status.

(29) Military Capabilities/Naval 2. Identify all surface, subsurface, or air contacts within 150 nautical miles of battle group.

(30) Military Capabilities/Naval 3. Detect, identify, classify, and track adversary surface warships.

(31) Military Capabilities/Naval 4. Detect, identify, classify, and track adversary submarines.

(32) Military Capabilities/Naval 5. Detect, locate, identify, classify, and track (time, position, course, speed) designated naval surface targets within adversary naval task force (include target description data, such as size, shape, and composition needed for weaponeering).

(33) Military Capabilities/Naval 6. Detect, locate, and characterize all other vessels capable of defending the target within 50 nautical miles of the target vessel, or other objects that may inhibit missile acquisition of the target.

(34) Military Capabilities/Naval 7. Identify, locate and describe country shore-based defensive positions, to include fixed and mobile antiship cruise missile systems, beach defenses, coastal artillery, coastal defense units, and coastal surveillance networks.

(35) Military Capabilities/Paramilitary. Describe country's paramilitary and/or indigenous forces, internal security forces or police (tables of organization and equipment, strength, type, number, capability, equipment, weapons, night operations).

(36) Military Capabilities/Rear Area Issues 1. Determine presence, location, strength, status, and identification of conventional forces isolated in friendly rear areas. Focus on those forces no longer controlled by higher HQ that could continue combat operations outside adversary's intent.

(37) Military Capabilities/Rear Area Issues 2. Detect, identify, and locate anti-US subversive elements within coalition force nations.

(38) Military Capabilities/Rear Area Issues 3. Describe adversary or sympathizers ability to infiltrate US deployment bases to conduct sabotage or subversive operations or attacks.

(39) Military Capabilities/Rear Area Issues 4. Detect presence, identity, location, strength, and activity of drug traffickers in the operational area.

(40) Military Capabilities/Rear Area Issues 5. Describe coalition and/or host nation foreign intelligence and security services' abilities to effectively collect and willingness to provide threat information in support of force protection efforts.

(41) Military Capabilities/Rear Area Issues 6. Describe the intelligence collection threat to friendly forces from foreign intelligence and security forces.

(42) Military Capabilities/SOF-Adversary 1. Determine presence, location, strength, doctrine, tactics, status, and identification of country SOF. Include paramilitary forces and elements which engage in sabotage, espionage, terrorism.

(43) Military Capabilities/SOF-Adversary 2. Determine country special operations and propaganda plans, programs, and capabilities.

(44) Military Capabilities/Space 1. Describe country's access to space-based intelligence systems or products. Identify types of products or systems and which country and/or consortium provides the access and/or products. Locate ground station downlinks.

(45) Military Capabilities/Space 2. Assess country's ability to deny US use of space systems.

(46) Military Capabilities/Surface-to-Surface Missiles (SSMs) 1. Describe, detect, classify by type, identify, and discriminate SSM or theater ballistic missiles (TBMs), particularly those with mobile launchers within range of the objective area.

(47) Military Capabilities/SSM 2. Detect, identify by type, and locate missile (SSM, TBM) launch event (friendly, threat, unknown):

(a) Locate, identify and track inflight theater missiles.

(b) Discriminate warhead type.

(c) Project impact point.

(d) Impact time and/or place, effect.

(48) Military Capabilities/SSM-Antiship. Detect, identify, classify, and track country SSM and/or antiship missiles within range of the naval task force. Detect and identify antishipping launches within the AOR and/or JOA.

(49) Military Capabilities/Training and Readiness 1. Assess general training level of country military units. Assess general level of military equipment maintenance and/or repair.

(50) Military Capabilities/Training and Readiness 2. Describe the readiness posture of military forces, both hostile and friendly, in the AOR and/or JOA.

(51) Military Capabilities/Weapons. Describe weapon systems and major military equipment items (both indigenous and foreign). Include type, availability, performance characteristics, strengths, vulnerabilities, maintenance and logistic capabilities, suppliers, training.

dd. **Military/General.** Describe uniform and equipment markings of the adversary, allies and coalition partners, and UN forces.

ee. **Military/Intentions or Strategy**

(1) Military/Intentions or Strategy 1. Assess adversary force leadership's intentions (attack, defend, withdraw, reinforce, or delay). Determine adversary commander's campaign plan. Describe adversary's military strategy.

(2) Military/Intentions or Strategy 2. Assess adversary radical employment of "last ditch" weapons or tactics.

ff. **Military/Occupation Policy.** Identify measures military forces have implemented in occupied areas for physical and operations security and to control the local population and resources. Identify incidents which have occurred between occupation forces and the local population.

gg. **Noncombatant Evacuation Operation.** Update noncombatant evacuation operation personnel information and adversary counter-tactics. Determine permissive, uncertain, or hostile environment.

hh. **Personnel**

(1) Personnel/Allied. Locate, identify and determine status of allied prisoners of war, hostages, and diplomats.

(2) Personnel/EPW. Estimate how many adversary troops will surrender. Describe their general medical condition, available food supplies, morale, and ability or will to resist EPW controls.

(3) Personnel/Morale 1. Determine the health of opposing forces. Describe degree of nutrition, affects of local diseases, extreme environmental conditions and flora and fauna which adversely affects their health. Determine the causes and impact of health issues upon their unit's mission and capabilities.

(4) Personnel/Morale 2. Determine morale of adversary military forces; thoughts about the war; opinion of their military and political leadership; opinion of military capability and resolve of the United States. Determine the impact of this morale upon unit mission and capabilities.

(5) Personnel/Morale 3. Identify military units which are experiencing discipline problems and determine the causes. Assess how this will impact their mission.

(6) Personnel/Morale 4. Identify social, cultural, ethnic, religious, or political friction or animosities which exist among adversary military personnel.

(7) Personnel/Morale 5. Determine what the civilian and military personnel of the host nation think of the United States, of other coalition forces' personnel and government, and of the military forces in their country. Describe any incidents of internal subversion against US forces or personnel or coalition forces or personnel.

(8) Personnel/Neutrals. Locate, identify and determine status of US travelers, such as students, journalists, or businessmen.

ii. **Psychological Operations.** Determine success of US or other friendly PSYOP product dissemination. Assess target audience behavior change for impact indicators and measures of effectiveness.

jj. **Public Affairs.** Determine releasability of operations information (unclassified) to the media.

kk. **Sea Mines and Obstacles**

(1) Sea Mines and Obstacles 1. Describe mine warfare capability.

(2) Sea Mines and Obstacles 2. Detect, locate, and classify by type and number, surface, subsurface, or land mines and obstacles within vicinity of naval task force or designated landing beaches.

(3) Sea Mines and Obstacles 3. Locate and track untethered live sea mines.

ll. **Special Operations Forces**

(1) Special Operations Forces/US 1. Provide support to prioritize SOF targets and selection of ingress and/or egress routes.

(2) Special Operations Forces/US 2. Determine possible effective PSYOP techniques.

mm. **Space.** Determine if threat nation is exploiting US satellite systems for any military-related system.

(1) Identify the adversary's reliance on space-based capabilities (i.e., navigation, satellite communications, weather, ISR, etc) to include those systems owned by the adversary or available from other nations.

(2) Identify the adversary's key satellite uplink and downlink stations.

nn. **Intertheater Lift.** Determine the status of LOCs connecting US and/or coalition forces with allies and/or supply nodes.

oo. **Targets**

(1) Targets 1. Determine country strategic and operational COGs.

(2) Targets 2. Identify, locate, describe, and prioritize fixed and mobile targets. Include critical strategic, operational and tactical facilities, airfields, offensive and defensive weapons systems, C4I facilities, troop concentrations, and other items of interest.

(3) Targets 3. Assess target vulnerabilities.

(4) Targets 4. Determine effect (possible political, economic, or sociological impact) of damage or destruction of the target on the populace or the country's warmaking potential.

(5) Targets 5. Provide comprehensive list and geographical position of all protected facilities such as hospitals, religious shrines, art treasures.

(6) Targets 6. Determine which specific transportation, media, industrial, communications, or other infrastructures need to be protected for intelligence purposes, for the restoration and/or restructuring phase, or for use by US and/or coalition forces.

(7) Targets 7. Provide target identification, including target name, mission number, Basic Encyclopedia number, target coordinates, category codes, safe area number, and country.

(8) Targets 8. Provide contingency targeting and associated planning materials, to include imagery, maps, charts, and target descriptions. Provide updates during conflict.

(9) Targets 9. Nominate target sets designed to avoid violations of war termination agreements (postconflict).

(10) Targets/Acquisition. Identify unique characteristics in target appearance and objects in target vicinity that contribute to or inhibit accurate scene generation for target acquisition (include varying weather, lightning, and seasonal conditions).

(11) Targets/Area Activity. Describe area activity on target (daily, weekly, monthly, seasonal, operational routine), and in target vicinity (daily, weekly, monthly, seasonal, operational routine in civilian neighborhood, industrial complex, business).

(12) Targets/Communications and Information Infrastructure. Describe target communications and information infrastructure to include type (telephone, radio, satellite communications, data fax, computer to computer); information security methods and procedures; visual signals or noise; and facilities (switches, power, antenna arrays, cables, personnel).

(13) Targets/Physical Description 1. Describe target physical layout or functional organization key component list, critical damage, or stress point.

(14) Targets/Physical Description 2. Describe target facility construction, type material, strength of walls, depth of walls, and effects of different types of munitions on facility.

(15) Targets/Power Sources. Describe target, primary and alternate power sources (number, type, location, conduits location, and type); associated facilities (transformers, switches, yards, relays, spares); fuel supply (types above and below, or partially below, ground location).

(16) Targets/Security. Locate target security posts, bunkers, trenches, and describe target security procedures to include patrols, lighting, detection systems, barriers and obstacles, entry, internal procedures, and personnel access.

(17) Targets/Security Forces. Describe adversary ground reaction capability to defend target, to include dedicated or incidental capabilities (strength, equipment, training, weapons, reaction time).

pp. **Terrorism/Narcotics.** Describe terrorist- or narcotics-related threats that jeopardize combatant command OPLANs. Include adversary or supporting groups and organizations; likely areas of operation or targets; tactics and methods; training areas; and hideouts.

qq. **Threat**

(1) Threat 1. Determine threat to US personnel and advisors.

(2) Threat 2. Identify safe houses (disposition, size and location).

rr. **WMD**

(1) WMD 1. Determine if the country possesses and if it will use WMD.

(2) WMD 2. Identify and classify facilities used for production or storage of WMD. Locate, identify, and classify threats, precise location of suspected weapon fabrication, assembly, and storage required.

(3) WMD 3. Describe the posture and disposition of country's WMD weapons, munitions, delivery systems, and units. Assess all potential types of WMD delivery systems, including biological vectors such as insects, animals, and infected humans. Confirm or deny presence of, and locate and identify, offensive WMD warfare-capable units. Characterize and determine types and quantities of WMD possessed by the country.

(4) WMD 4. Identify the locations and types of WMD defense-related facilities and capabilities (e.g., individual and collective protection, medical, and decontamination).

(5) WMD 5. Identify terrorist organizations acting alone or with state sponsorship that possess or are attempting to acquire WMD.

ss. **Toxic Industrial Materials.** Identify commercial facilities (chemical, bio-pharmaceutical, using or producing radioisotopes, nuclear facilities) that either through accident, wartime collateral damage, or terror/sabotage, could release TIMs.

APPENDIX D
SAMPLE INTELLIGENCE ESTIMATE FORMAT

INTELLIGENCE ESTIMATE

SECURITY CLASSIFICATION

Originating Section Issuing HQ*
Place of Issue
Day, Month, Year, Hour, Zone

INTELLIGENCE ESTIMATE NUMBER**

( ) REFERENCES: a. Geospatial products and services.
b. Other relevant documents.

1. ( ) Mission. State the assigned task and its purpose. The mission of the command as a whole is taken from the commander's mission analysis, planning guidance, or other statement.

2. ( ) Adversary Situation. State conditions that exist and indication of effects of these conditions on adversary capabilities and the assigned mission. This paragraph describes the operational area, the adversary military situation, and the effect of these two factors on adversary capabilities.

a. ( ) Characteristics of the Operational Area. Discuss the effect of the physical characteristics of the operational area on military activities of both combatants. If an analysis of the area has been prepared separately, this paragraph in the intelligence estimate may simply refer to it, then discuss the effects of the existing situation on military operations in the area.

(1) ( ) Military Geography

(a) ( ) Topography

* When this estimate is distributed outside the issuing HQ, the first line of the heading is the official designation of the issuing command, and the ending of the estimate is modified to include authentication by the authorizing section, division, or other official according to local policy.

** Normally, these are numbered sequentially during a calendar year.

SECURITY CLASSIFICATION

SECURITY CLASSIFICATION

1. ( ) Existing Situation. Describe relief and drainage, vegetation, surface materials, cultural features and other characteristics in terms of their effect on key terrain, observation, fields of fire, obstacles, cover and concealment, avenues of approach, LOCs, and landing areas and zones.

2. ( ) Effect on Adversary Capabilities. Discuss the effect of topography on broad adversary capabilities such as attack and defense, describing generally how the topography affects each type of activity. The effect of topography on the employment of WMD; amphibious, airborne, or air-landed forces; surveillance devices and systems; communications equipment and systems; EW; PSYOP, including source, content, audience, media, and effectiveness; OPSEC and military deception; logistic support; and other appropriate considerations should be included.

3. ( ) Effect on Friendly COAs. Discuss the effects of topography on friendly forces' military operations (attack, defense) in the same fashion as for adversary capabilities in the preceding subparagraphs.

(b) ( ) Hydrography

1. ( ) Existing Situation. Describe the nature of the sea and the coastline within the amphibious objective area; adjacent islands; location, extent, and capacity of landing beaches and their approaches and exits; nature of the offshore approaches, including type of bottom and gradients; natural obstacles; surf, tide, and current conditions.

2. ( ) Effect on Adversary Capabilities. Discuss the effects of the existing situation on broad adversary capabilities.

3. ( ) Effect on Friendly COAs. Discuss the effects of the existing situation on broad COAs for friendly forces.

(c) ( ) Climate and Weather

1. ( ) Existing Situation. Describe temperature, cloud cover, visibility, precipitation, light data, and other climate and weather conditions and their general effects on roads, rivers, soil trafficability, and observation.

2. ( ) Effect on Adversary Capabilities. Discuss the effects of the existing climate and weather situation on broad adversary capabilities.

3. ( ) Effect on Friendly COAs. Discuss the effects of the existing climate and weather situation on broad COAs for friendly forces.

SECURITY CLASSIFICATION

SECURITY CLASSIFICATION

(2) ( ) Transportation

(a) ( ) Existing Situation. Describe roads, railways, inland waterways, airfields, and other physical characteristics of the transportation system; capabilities of the transportation system in terms of rolling stock, barge capacities, and terminal facilities; and other pertinent data.

(b) ( ) Effect on Adversary Capabilities. Discuss the effects of the existing transportation system and capabilities on broad adversary capabilities.

(c) ( ) Effect on Friendly COAs. Discuss the effects of the existing transportation system and capabilities on broad COAs for friendly forces.

(3) ( ) Telecommunications

(a) ( ) Existing Situation. Describe telecommunications facilities and capabilities in the area.

(b) ( ) Effect on Adversary Capabilities. Discuss the effects of the existing telecommunications situation on broad adversary capabilities.

(c) ( ) Effect on Friendly COAs. Discuss the effects of the existing telecommunications situation on broad COAs for friendly forces.

(4) ( ) Politics

(a) ( ) Existing Situation. Describe the organization and operation of civil government in the operational area.

(b) ( ) Effect on Adversary Capabilities. Consider the effects of the political situation on broad adversary capabilities.

(c) ( ) Effect on Friendly COAs. Consider the effects of the political situation on broad COAs for friendly forces.

(5) ( ) Economics

(a) ( ) Existing Situation. Describe industry, public works and utilities, finance, banking, currency, commerce, agriculture, trades and professions, labor force, and other related factors.

SECURITY CLASSIFICATION

SECURITY CLASSIFICATION

(b) ( ) Effect on Adversary Capabilities. Discuss the effects of the economic situation on broad adversary capabilities.

(c) ( ) Effect on Friendly COAs. Consider the effects of the economic situation on broad COAs for friendly forces.

(6) ( ) Sociology

(a) ( ) Existing Situation. Describe language, religion, social institutions and attitudes, minority groups, population distribution, health and sanitation, and other related factors.

(b) ( ) Effect on Adversary Capabilities. Discuss the effects of the sociological situation on broad adversary capabilities.

(c) ( ) Effect on Friendly COAs. Discuss the effects of the sociological situation on COAs for friendly forces.

(7) ( ) Science and Technology

(a) ( ) Existing Situation. Describe the level of science and technology in the operational area.

(b) ( ) Effect on Adversary Capabilities. Discuss the effects of science and technology on broad adversary capabilities.

(c) ( ) Effect on Friendly COAs. Discuss the effects of science and technology on broad COAs for friendly forces.

b. ( ) Adversary Military Situation (ground, naval, air, space, and special operations)

(1) ( ) Strength. State the number and size of adversary units committed and adversary reinforcements available for use in the operational area. Ground strength, air power, space capabilities, naval forces, WMD, EW, UW, special operations, surveillance potential, and all other strengths (which might be significant) are considered.

(2) ( ) Composition. Outline the structure of adversary forces (OB) and describe unusual organizational features, identity, armament, and weapon systems.

SECURITY CLASSIFICATION

SECURITY CLASSIFICATION

(3) ( ) Location and Disposition. Describe the geographic location of adversary forces in the area, including fire support elements; C2 facilities; air, naval, and missile forces; and bases.

(4) ( ) Availability of Reinforcements. Describe adversary reinforcement capabilities in terms of ground, air, naval, missile, and WMD forces and weapons, terrain, weather, road and rail nets, transportation, replacements, labor forces, prisoner of war policy, and possible aid from sympathetic or participating neighbors.

(5) ( ) Movements and Activities. Describe the latest known adversary activities in the area.

(6) ( ) Logistics. Describe levels of supply, resupply ability, and capacity of beaches, ports, roads, railways, airfields, and other facilities to support supply and resupply. Consider hospitalization and evacuation, military construction, labor resources, and maintenance of combat equipment.

(7) ( ) Operational Capability to Launch Missiles. Describe the total missile capability that can be brought to bear on forces operating in the area, including characteristics of missile systems, location and capacity of launch or delivery units, initial and sustained launch rates, size and location of stockpiles, identification of critical launch support elements, and other pertinent factors.

(8) ( ) Serviceability and Operational Rates of Aircraft. Describe the total aircraft inventory by type, performance characteristics of operational aircraft, initial and sustained sortie rates of aircraft by type, and other pertinent factors.

(9) ( ) Operational Capabilities of Combatant Vessels. Describe the number, type, and operational characteristics of ships, boats, and craft in the naval inventory; base location; and capacity for support.

(10) ( ) Technical Characteristics of Equipment. Describe the technical characteristics of major items of equipment in the adversary inventory not already considered (such as missiles, aircraft, and naval vessels).

(11) ( ) Collection Capabilities. Describe the adversary intelligence-gathering capability using any of the intelligence collection disciplines (SIGINT, IMINT, HUMINT, MASINT).

(12) ( ) IO. Describe the adversary offensive and defensive IO capabilities.

SECURITY CLASSIFICATION

SECURITY CLASSIFICATION

(13) ( ) WMD. Describe the types and characteristics of WMD in the adversary inventory, stockpile data, delivery capabilities, WMD employment policies and techniques, potential for starting biological warfare epidemics, locations of TIM, and other pertinent factors.

(14) ( ) Significant Strengths and Weaknesses. Discuss the significant adversary strengths and weaknesses perceived from the facts presented in the preceding subparagraphs.

c. ( ) Adversary Unconventional and Psychological Warfare Situation

(1) ( ) Guerrilla. Describe the adversary capability for, policy with regard to, and current status in the area of guerrilla or insurgent operations.

(2) ( ) Psychological. Describe adversary doctrine, techniques, methods, organization for, and conduct of propaganda in the operational area.

(3) ( ) Subversion. Describe adversary doctrine, techniques, methods, organization for, and conduct of subversion in the operational area.

(4) ( ) Sabotage. Outline adversary organization and potential for and conduct of sabotage in the operational area.

3. ( ) Adversary Capabilities

a. ( ) List each adversary capability that can affect the accomplishment of the assigned mission. Each adversary capability should contain information on the following:

(1) ( ) What the adversary can do.

(2) ( ) Where they can do it.

(3) ( ) When they can start it and get it done.

(4) ( ) What strength they can devote to the task.

b. ( ) In describing adversary capabilities, the J-2 must be able to tell the commander what the adversary can do using its forces in a joint environment. First, of course, the J-2 must assess the adversary's ground, naval, and air forces. It is customary to enumerate separately the WMD, UW, space, and special operations capacities. Hypothetical examples follow.

SECURITY CLASSIFICATION

SECURITY CLASSIFICATION

(1) ( ) Ground Capabilities

(a) ( ) The adversary can attack at any time along our front with an estimated 6 infantry divisions and 2 tank divisions supported by 24 battalions of artillery.

(b) ( ) The adversary can defend now in its present position with 7 infantry divisions supported by 2 tank divisions and 16 battalions of medium and light artillery.

(c) ( ) The adversary can reinforce its attack (or defense) with all or part of the following units in the times and places indicated:

UNIT	PLACE	TIME
315th Airborne Div	Vic RESOGA	8 hrs after starting time
41st Motorized Div	Vic CARDINAL	6 hrs after starting time

(2) ( ) Air Capabilities

(a) ( ) Starting now, and based on an estimated strength of 300 fighters and 100 medium bomber aircraft, the adversary can attack in the operational area with 240 fighter sorties per day for the first 2 days, followed by a sustained rate of 150 sorties per day, and 60 bomber sorties per day, for 1 day followed by a sustained rate of 48 sorties per day.

(b) ( ) Using airfields in the vicinity of ____, the adversary has sufficient transport sorties to lift one regiment in a single lift to airfields in the vicinity of ____ and ____ within 4 hours' flying time.

(3) ( ) Naval Capabilities. Starting now, the adversary can conduct sustained sea and air operations in the entire area with 6 DDs, 4 FFs, 1 CV, 7 SSNs, a mine force of 20 craft, and 70 gunboats and smaller craft now on station in the area.

(4) ( ) Nuclear and Radiological Capabilities. The adversary can employ at any time and in any part of the operational area an estimated 40 to 60 nuclear weapons of yields from 2 to 50 kt delivered by cannon and rocket artillery, guided missile, and aircraft. The adversary has delivered radiological materials to supporting terrorist teams who have assembled up to 6 radiological dispersal devices.

SECURITY CLASSIFICATION

SECURITY CLASSIFICATION

(5) ( ) Biological and Chemical Capabilities. The adversary can employ the chemical agents ____, ____, and ____ in the operational area at any time delivered by air, cannon, and rocket artillery and by guided missile. Weaponized anthrax can be delivered by remotely piloted vehicles and by terrorist suicide teams into crowded civilian areas next to military installations. Suicide teams may also infect themselves with a communicable disease and attempt to mingle with US, allied, and host nation personnel.

(6) ( ) UW Capability. The adversary can conduct UW operations in the area within 10 days after starting the operation using dissident ethnic elements and the political adversaries of the current government.

(7) ( ) Joint Capabilities. The adversary can continue to defend its present position with 6 infantry divisions, supported by 16 artillery battalions and reinforced by 3 mechanized divisions within 8 hours after starting movement. Adversary defense also can be supported by 150 fighter sorties daily for a sustained period and by continuous naval surface and air operations employing 6 DDs, 4 FFs, 7 SSNs, and 1 CV.

4. ( ) Analysis of Adversary COAs. Analyze each adversary capability in light of the assigned mission (considering all applicable factors from paragraph 2 above) and attempt to determine COAs and their relative order of probability of adoption by the adversary. Discuss adversary vulnerabilities. In this paragraph, examine each adversary COA by discussing the factors that favor or militate against its adoption by the adversary. When applicable, the analysis of each COA should also include a discussion of adversary vulnerabilities attendant to that COA (i.e., conditions or circumstances of the adversary situation that render the adversary especially liable to damage, deception, or defeat). Finally, the analysis should include a discussion of any indications that point to possible adoption of the COA, as in the following:

a. ( ) Attack now with forces along the forward edge of the battle area _____

(1) ( ) The following factors favor the adversary's adoption of this capability:

(a) ( ) _____

(b) ( ) _____

(2) ( ) The following factors militate against the adversary's adoption of this capability:

SECURITY CLASSIFICATION

SECURITY CLASSIFICATION

(a) ( ) Road and rail nets will not support large-scale troop and supply movements necessary for an attack in the area.

(b) ( ) Terrain in the area does not favor an attack.

(3) ( ) Adoption of this capability will expose the adversary's west flank to counterattack.

(4) ( ) Except for minor patrol activity in the _____ area, there are no indications of adoption of this capability.

b. ( ) Delay from present positions along the _____ River line _____

(1) ( ) The following factors favor the adversary's adoption of this capability:

(a) ( ) There are several excellent natural barriers between the _____ River and the _____ Mountains.

(b) ( ) The effectiveness of the water barriers will improve, and trafficability on the upland slopes of the terrain barriers will deteriorate with advent of the monsoon.

(2) ( ) The following factors militate against the adversary's adoption of this capability:

(a) ( ) _____

(b) ( ) _____

(3) ( ) In the adoption of this capability, the adversary's LOCs will be restricted by a limited road and rail net that can easily be interdicted.

(4) ( ) The following facts indicate adoption of this capability:

(a) ( ) Aerial photography indicates some preparation of barriers in successive positions.

(b) ( ) Considerable troop movement and prepositioning of floating bridge equipment along the water barriers have been detected.

SECURITY CLASSIFICATION

SECURITY CLASSIFICATION

5. ( ) Conclusions. Conclusions resulting from discussion in paragraph 4 above. Include, when possible, a concise statement of the effects of each capability on the accomplishment of the assigned mission. Cite adversary vulnerabilities where applicable. This paragraph contains a summary of adversary capabilities most likely to be adopted, listed in the order of relative probability if sufficient information is available to permit such an estimate. If appropriate, it should also include a concise statement of the effects of each adversary capability on the accomplishment of the assigned mission. Exploitable vulnerabilities should also be listed, where applicable.

a. ( ) Adversary Capabilities in Relative Probability of Adoption

(1) ( ) Defend in present locations with _____

(2) ( ) Delay from present positions along _____

(3) ( ) Reinforce the defense or delay with _____

(4) ( ) Conduct UW operations in the area _____

b. ( ) Vulnerabilities

(1) ( ) Adversary left (west) flank is open to envelopment by amphibious assault._____

(2) ( ) The adversary's air search radar coverage is poor in the left (west) portion of its defensive sector _____

(Signed) _____
J-2

(The staff division chief signs the staff estimates produced by that division. If the estimate is to be distributed outside the HQ, the heading and signature block must be changed to reflect that fact.)

ANNEXES: (By letter and title) Annexes should be included where the information is in graphs or of such detail and volume that inclusion makes the body of the estimate cumbersome. They should be lettered sequentially as they occur throughout the estimate.

DISTRIBUTION: (According to procedures and policies of the issuing HQ)

SECURITY CLASSIFICATION

APPENDIX E
SECURITY

1. Overview

a. Security doctrine and procedures safeguard and protect lives, information sources, and operations, and facilitate the timely movement and/or flow and dissemination of raw data and finished intelligence. All intelligence operations are dependent upon the proper implementation and enforcement of security procedures to prevent violations and compromises, and to provide valuable time-sensitive intelligence to commanders. In a crisis situation, especially in a multinational environment, the J-2 must continue to maintain and enforce thorough and effective security procedures.

b. The J-2 makes a major contribution to the success of operational missions through peacetime security planning and preparation of tailored support to potential operations as well as careful consideration of possible security-related contingencies. This preplanning is especially significant during MOOTW involving multinational forces, which complicates dissemination and releasability procedures. In all environments, the J-2 must consider and assess such issues as:

(1) Properly classifying and/or sanitizing intelligence material to ensure the timely flow of critical intelligence to the requester, while considering the security implications of intelligence exchanges; and

(2) Using effective CI to enhance deception planning and operations.

2. Personnel Security

a. Among intelligence professionals, vigilance is the watchword, and periodic security training for all personnel is the method used to stress awareness and rectify procedural deficiencies and shortcomings. Personnel security standards have been met if there is no reasonable basis for doubting the person's loyalty to the USG. Combatant commanders can grant interim clearances, administratively withdraw clearances, and grant or deny access to classified information per the guidelines contained in DODD 5200.2-R, *DOD Personnel Security Program*. The Services' senior officers of the IC (SOICs) or their designees may grant SCI access for their respective Military Departments. The Director, DIA is responsible for OSD, Joint Staff, the Defense agencies, and DOD field activities (less NSA/CSS and NRO).

b. An interlocking and mutually supporting series of program elements (e.g., need to know, investigation, binding contractual obligations on those granted access, security education and awareness, and individual responsibility) provides reasonable assurances against compromise of classified information. The primary security principle in safeguarding classified information is to ensure that it is accessible only by those persons with an appropriate clearance, access approval, clearly identified need to know, signed nondisclosure agreement, and an appropriate indoctrination (for SCI).

3. Sensitive Compartmented Information Facility

Before SCI can be handled, processed, or stored, a SCIF must be accredited based on established physical security guidelines. The SSO is the POC for information on accreditation authorities and SCIF physical security guidelines.

a. **Establishing and Accrediting a Temporary and/or Emergency SCIF**

(1) A SCIF at any level of accreditation may be established upon the verbal order of a general and/or commander during declared hostilities or general war. Reconciliation of SCIF activation and operational data will be made no more than 180 days after SCIF activation.

(2) For operational contingencies, and with prior DIA coordination, a SOIC may approve a temporary SCIF for up to 60 days. DIA will assign a SCIF identification number and retain authority to cancel, extend, or change the accreditation. There are no specific physical requirements for such a SCIF, although sound attenuation problems should be addressed, the SCIF should be staffed around-the-clock, and appropriate guards should monitor and/or patrol the area.

(3) A tactical SCIF is a military field operation established during crisis, contingency, or exercise. A tactical SCIF can be set up and temporarily accredited by a SOIC. This authority may be further delegated in writing to one lower level of command. The local approving authority may require use of a local tactical deployment checklist. The element authorizing establishment of a tactical SCIF notifies the accreditation authority and DIA by message before starting SCIF operations. The message format is shown in Figure E-1.

(4) A tactical SCIF may be operated within a randomly selected structure for the duration of an exercise. If reused within 36 months for SCI discussion, a technical surveillance countermeasures evaluation is recommended. During crisis and hostilities, there is no restriction over SCI discussion within a tactical SCIF.

(5) A temporary secure working area (TSWA) is a temporarily accredited facility used no more than 40 hours per month for handling or discussing SCI. SOICs and combatant command senior intelligence officers (SIOs) may approve TSWAs for all levels of SCI. SOICs, SIOs and DIA may approve electronic processing of SCI in a TSWA. Approval of temporary storage of SCI, not to exceed 6 months, may be granted by DIA or a Service.

(6) Shipboard SCIFs. A shipboard tactical facility requires submission of the shipboard accreditation checklist to the Navy accreditation authority. Temporary shipboard accreditation is approved by SOIC Navy for units which may deploy for emergency contingencies, not to exceed a 12-month deployment period. Permanent accreditation is approved by SOIC DIA.

(7) Aircraft SCIFs. Aircraft will be accredited through established accreditation channels. Transports and courier aircraft transporting SCI material between airfields do not require accreditation; however, compliance with SCI material and communications directives

SAMPLE TACTICAL SENSITIVE COMPARTMENTED INFORMATION FACILITY OPERATIONS MESSAGE FORMAT

FROM: (Originator's Message Address)
TO: SSO DIA/DAC-2A//
CLASSIFICATION
SUBJECT: TACTICAL SCIF OPERATION (U)

1. (U) DIA SCIF-ID number of parent SCIF.
2. (U) Name of Tactical SCIF.
3. (U) Deployed from location.
4. (U) Deployed to location.
5. (U) SCI level of operations.
6. (U) Operational period.
7. (U) Name of exercise or operation.
8. (U) Identification of facility used for SCIF operations (e.g., vans, buildings, tents).
9. (U) Points of contact.
10. (U) Description of security measures.
11. (U) Comments.
12. (U) POC FOR THE ACTION: (name, office symbol, and telephone number).

Figure E-1. Sample Tactical Sensitive Compartmented Information Facility Operations Message Format

are mandatory. Aircraft temporarily configured for SCI missions by installing pallets, vans, or containers aboard, will be accredited by the appropriate SOIC having SCI cognizance. Contingency and emergency deployment aircraft, operating with SCI processing aboard, may be operated as a tactical SCIF IAW DCID 1/21, *Physical Security Standards for SCIFs*.

b. **Tactical SCIF Security.** Although security is necessary for the integrity of a SCIF, the SSO determines the degree of security to be maintained, taking the operators' needs and the local situation into account. Security should support, rather than restrict, the mission. Recommended guidelines for maintaining SCIF security include the following:

(1) Staff the tactical SCIF with sufficient personnel as determined by the onsite security authority based on the local threat conditions.

(2) Locate the tactical SCIF within the supported HQ's defense perimeter.

(3) Post armed guards to protect the entire perimeter of the SCIF compound. Maintain radio or wire communications with the guard and reserve force.

(4) Use a single entrance and access control procedures.

(5) Keep emergency destruction and evacuation plans current and displayed.

(6) Store SCI materials in lockable containers when not in use.

(7) Incorporate the SCIF physical security plan into the perimeter defense plan.

(8) Store no more intelligence than can be destroyed in a reasonable amount of time.

c. **Assignments of Foreign Representatives to a SCIF.** Prior to the assignment of foreign personnel to a SCIF, the subordinate joint force J-2 must consider the scope of the foreigner's role in relation to the environment. Foreign representatives in a SCIF should be physically located so that they may work effectively without being inadvertently exposed to restricted data. If a tactical SCIF is in a multinational environment with a US-only area, the US-only area must be kept separate from any multinational operations. The guard(s) must be a US citizen. The J-2, in coordination with the SSO, should ensure constant oversight of nonintelligence elements residing in the SCIF to ensure that there will be no compromise of operational matters.

4. Sanitizing and/or Releasing Intelligence

a. USG policy is to treat classified military information as a national security asset, which may be shared with foreign governments and international organizations only when there is a clearly defined advantage to the United States. US national interests require that foreign governments provide US classified information with a degree of security protection comparable to what it would receive while under US control. There are a number of international and bilateral security agreements in effect to ensure this. However, in exceptional cases it will be in US interests to make information available to a foreign government before concluding an agreement, even if the recipient government's safeguards appear inadequate. In these cases, when authorized by the National Disclosure Policy Committee (NDPC) as exceptions to policy, a balance is sought between US national interests and the security of the classified information.

b. NDP-1, *National Defense Policy*, governs how the United States releases military information to foreign governments and international organizations and establishes eligibility criteria to receive releasable information. Detailed procedures for handling, processing, downgrading, release and sanitization of these materials exist. Key national security policy and security manuals are included in Appendix J, "References."

c. Intelligence information, even though it bears no restrictive control markings, may only be released in its original form to foreign governments or international organizations with the permission of the originator and IAW DCID 6/7, *Intelligence Disclosure Policy*, and NDP-1, *National Defense Policy*. Information contained in intelligence products or reports of another IC component, which bears no restrictive control markings, may be used by recipient IC components in reports provided to foreign governments under the following conditions:

(1) Foreign release occurs through established foreign disclosure and procedures.

(2) No reference is made to the originating agency or to the source documents upon which the released product is based.

(3) The information is extracted or paraphrased to ensure that the source or manner of acquisition of the intelligence and/or location where the intelligence was collected (if relevant to protect sources or methods) is not revealed and cannot be deduced in any manner.

(4) RESTRICTED DATA and FORMERLY RESTRICTED DATA are prohibited from foreign dissemination under the provisions of Public Law 585, Atomic Energy Act of 1954, as amended.

d. Even though it bears no restrictive control markings, intelligence will not be released, either in its original form or otherwise, to foreign nationals or immigrant aliens (including those employed by, used by, or integrated into the USG) without the permission of the originator and IAW DCID 6/7*, Intelligence Disclosure Policy*, and NDP-1, *National Defense Policy*.

e. An SSO can provide more detailed information on SCI policy and procedures, and the DISO assigned to the cognizant combatant command can help to seek exemptions to security policy from national agencies. The combatant commander is responsible for the release of intelligence and should request that intelligence producers tailor their product so as to minimize the use of caveats.

f. As shown in Figure E-2, and apart from the exceptions listed in Figure E-3, military information is divided into eight functional categories by the NDPC. In almost all cases, intelligence under consideration for release at the subordinate joint force J-2 level will be in Category 8. Combatant command requests for disclosure of NDPC-exception categories of intelligence information will be made IAW the policies and directives of the DOD, IC members, or other office responsible for the information.

g. Classified information may only be disclosed when the following applies:

(1) Disclosure is consistent with US foreign policy and national security objectives concerning the recipient foreign government or international organization.

(2) Disclosure can be expected to result in a clearly identifiable advantage to the United States.

(3) It can be reasonably assumed that the disclosed information would not be used against US interests.

h. Release Policies and Procedures. J-2s should consider the following when determining whether to release classified information:

Figure E-2. National Disclosure Policy Functional Categories of Classified Military Intelligence

(1) Determine recipient country's eligibility to receive military intelligence. If the country is not eligible yet meets the conditions listed below, a request for exemption to NDP can be made through the combatant command's foreign disclosure officer.

(2) Determine recipient's need to know. Any recipient, whether a member of the US military or a foreign government, must have a "need to know" before being provided with US intelligence. While determining need may be difficult, the J-2 may rely on common sense and knowledge of the situation. For example, Country X has a legitimate need to know about Country Y-sponsored terrorist activities in the region. However, since Country X faces no direct military threat from Country Y, it has no need to know and is not eligible to receive information on Country Y's OB. Where necessary, a decision may be based on political and/or military expediency.

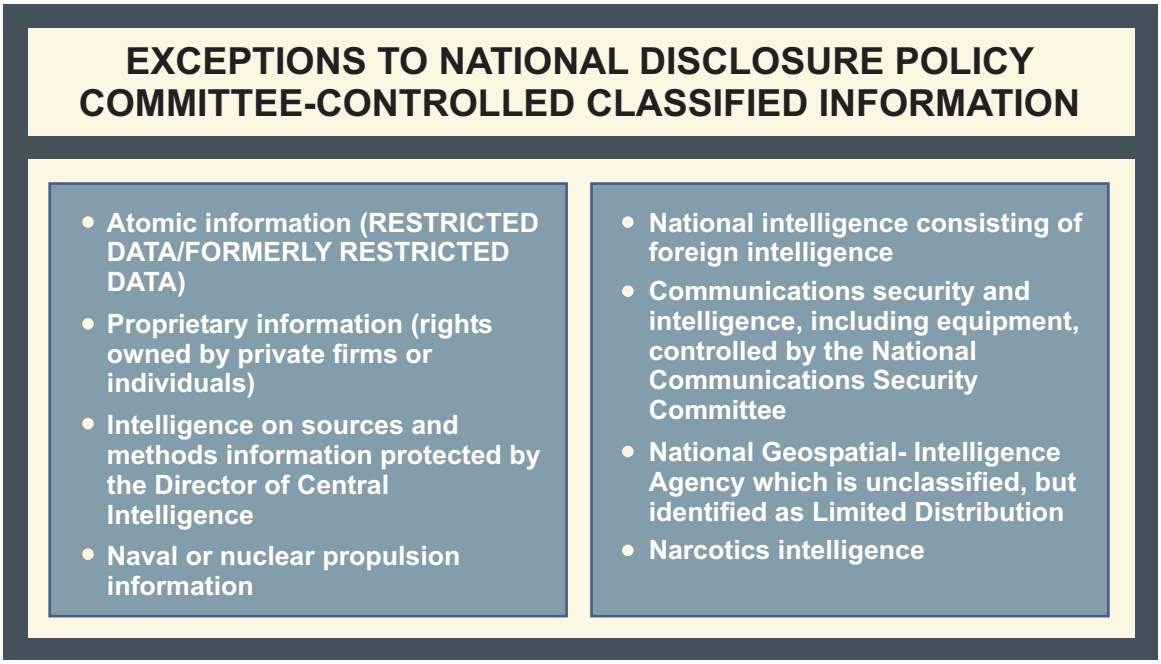


Figure E-3. Exceptions to National Disclosure Policy Committee-Controlled Classified Information

(3) The gain must clearly outweigh the risk of compromising the source. This is most easily ensured by sanitizing the original report to protect the source.

(4) Release intelligence only to the level of command necessary, as determined by the J-2.

(5) As noted above, except in exceptional circumstances, the organization receiving the intelligence must reasonably be expected to afford the same degree of protection against compromise as would US channels.

i. Key points on release of classified material are listed in Figure E-4.

5. Information Systems Security

a. The authority to permit the automated processing of intelligence information is vested in the Director, DIA, who has the responsibility to ensure that the risks posed during processing are outweighed by the gain. Specifically, this means that adequate security of contractor and DOD (less NSA/CSS) automated information systems and the security of systems (networks) that store, process and/or transmit sensitive foreign intelligence information, are under the cognizance of the Director, DIA. DIA manages the DODIIS Computer Security Program IAW the appropriate DOD and DCI directives.

b. As far in advance of joint operations as possible, personnel responsible for establishing security (in coordination with those responsible for determining the information system and/or connectivity requirements) should contact DIA. They must inform DIA of the names and accreditation status of

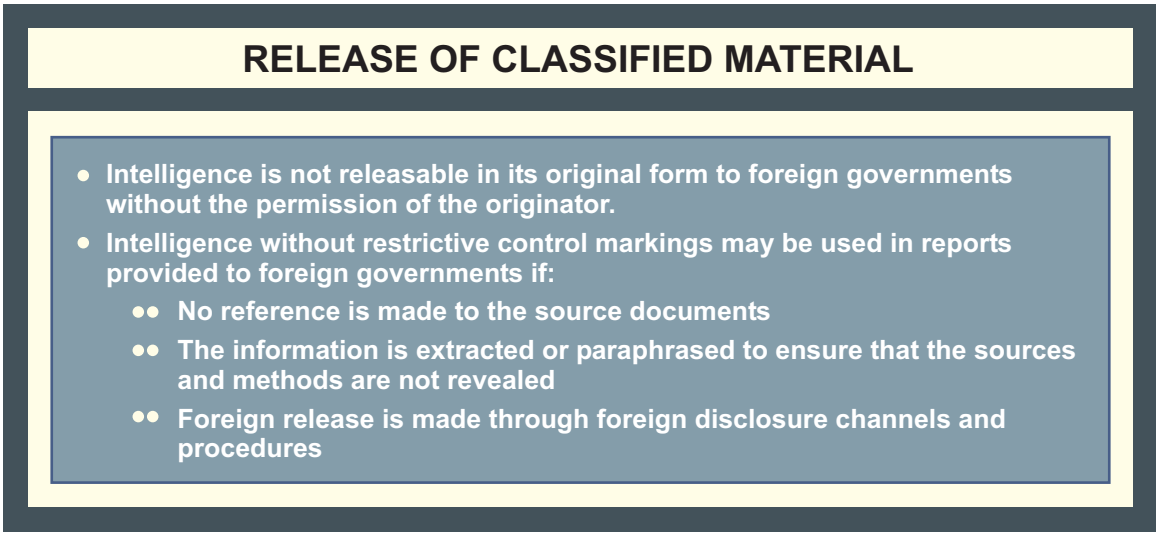


Figure E-4. Release of Classified Material

systems to be used during the operation, as well as planned inter-connectivity. DIA will work with planners to balance security requirements with operational requirements.

APPENDIX F
DEPARTMENT OF DEFENSE SHARED PRODUCTION PROGRAM

1. Introduction

The DODIPP was established in response to Congressional mandate to reduce duplication of effort within the DODIPC. Central to the DODIPP concept is the sharing of production. Production responsibilities are assigned to capitalize on the analytical and production resources of the entire DODIPC to focus expertise and maximize output for the consumer. The structure is an explicit, logical division of activities, responsibilities, and accountability among national, Service, and combatant command production centers based on traditional roles as specified in Title 10 United States Code and the national-level military intelligence requirements forums. The SPP is based on databases produced by two or more intelligence production centers. These producers are responsible for all production based on the substantive topics in the shared database.

2. Responsibilities

a. In the event of a crisis or war, defense production support will focus on the NMJIC, which will form intelligence work groups or intelligence task forces as necessary IAW designated responsibilities and procedures. RFIs/PRs from the crisis and/or engaged joint force will be transmitted to its combatant command VO which, if unable to satisfy the RFI/PR, will forward it to the NMJIC. All other RFIs/PRs relating to the crisis will be forwarded through normal VO chains of command to the NMJIC, which will be the single DOD VO for all other RFIs/PRs related to the crisis.

b. The Defense Intelligence Production Functional Manager is responsible for ensuring that DODIPC production supports the NMJIC during a crisis or conflict. The NMJIC will have the authority to assign PRs and reprioritize ongoing crisis-related production in coordination with the combatant commands. The Defense Intelligence Production Functional Manager will retain oversight of noncrisis-related DODIPC production, adjusting production schedules as necessary.

c. The Director, DI acts as the executive agent for production issues for the Director, DIA. Key responsibilities (for a complete list of responsibilities, see DOD-0000-151-YR, *DOD Intelligence Production Program*) include the following:

(1) Evaluate DODIPP production center production and capabilities in conjunction with the combatant commands, Services, and appropriate Defense agencies through production program reviews at each DODIPC production center.

(2) Assign and change DODIPP responsibilities as required in coordination with the appropriate combatant command, Service, and Defense agency representatives.

(3) Assist production centers in developing needed capabilities; identify, coordinate, and program resource requirements to meet DODIPP responsibilities; and serve as an advocate for SPP resource planning and application.

(4) Initiate management coordination when problems arise, and mediate disagreements.

(5) Manage the coordination of SPP database requirements and specifications to establish DOD-wide standards for applicable data elements, documentation, and communications. Provide implementation guidance and schedules for approved changes and monitor implementation.

(6) Maintain active, continuous, and meaningful communication with production centers on improving the production of substantive intelligence.

(7) Act as advocate for collection requirements to support the currency and validity of SPP production.

d. Based on DODIPP guidelines, Military Service intelligence chiefs are charged with the same responsibilities as the combatant commands for DODIPP tasks through Service channels (for a complete list of responsibilities see DOD-0000-151-YR, *DOD Intelligence Production Program*) to include the following:

(1) Validating requirements and producing intelligence to satisfy Title 10 responsibilities in support of the Service Secretaries' responsibilities.

(2) Coordinating and accomplishing planning, programming, and budgetary actions to support the SPP, including analytical, automated intelligence system and telecommunication capability requirements identified by production centers and supported commands.

(3) Ensuring that adequate training capabilities are available for current and future analytical intelligence personnel to support production responsibilities.

APPENDIX G
JOINT EXPLOITATION CENTERS

1. Overview

a. The exploitation of captured adversary material and the interrogation and debriefing of EPWs, ECs, detainees, refugees, and other displaced persons provides significant collection opportunities. The information obtained through this exploitation, coupled with that derived from other collection assets, will provide the JFC (through the J-2) a more complete picture of the operational environment and, potentially, adversary capability and intentions. The in-theater exploitation of these sources is accomplished at three centers (see Figure G-1).

(1) Joint captured materiel exploitation center.

(2) Joint document exploitation center.

(3) Joint interrogation and debriefing center.

b. Short-term exploitation of captured equipment and documents as well as interrogation or debriefing of EPWs, ECs, refugees, and other sources may be of immediate tactical value. Such debriefings can provide information important for decisions regarding the targeting cycle and tempo of operations; therefore, tactical exploitation by trained intelligence personnel must

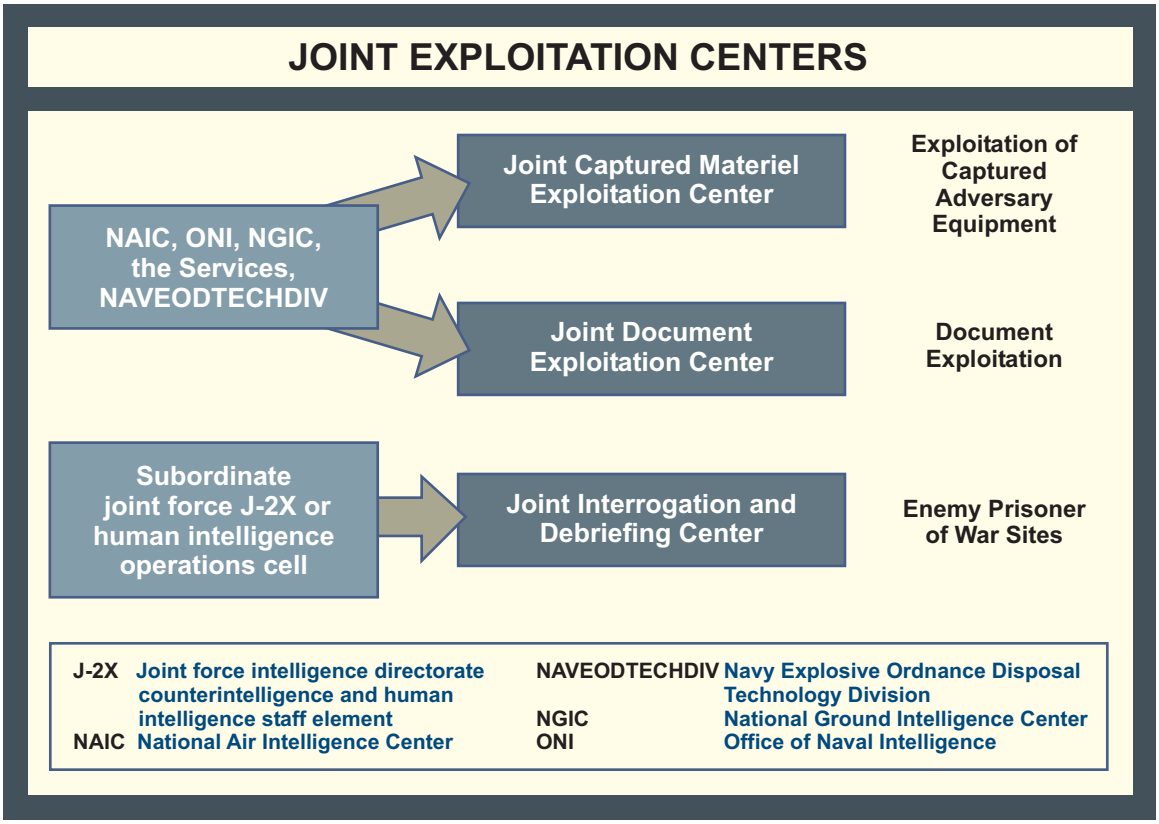


Figure G-1. Joint Exploitation Centers

be accomplished as soon as possible and at the lowest possible tactical level. Long-term exploitation of the same material and sources at joint force level provides valuable operational, strategic, and technical data, and at a greater fidelity than otherwise possible. Further exploitation may be continued out of theater where there are better facilities for detailed research and analysis.

c. Whenever possible the JCMEC, JDEC, and JIDC should be collocated in an intelligence exploitation base at the joint force component level to facilitate rapid exchange of data. Although these three centers conduct exploitation in the AOR and/or JOA, their functions are not limited solely to combat support. Both peacekeeping operations and refugee relief, for example, could require confiscating weapons and contraband; and refugee relief could also require screening refugees for critical information. In MOOTW, the names of these centers may be changed to reflect the type of operations being supported while the functions remain the same.

2. Joint Captured Materiel Exploitation Center

The recovery of CEE is both a combatant command and a national requirement. Subsequent exploitation of this material provides critical information on adversary strengths and weaknesses that may favorably influence operation planning and force protection. Furthermore, the acquisition of foreign material satisfies national-level requirements of the Service intelligence centers for S&TI. The identification, recovery, in-theater analysis, and evacuation of this material is done by the JCMEC. Combatant commands or subordinate joint forces should notify the NMJIC through command channels that they require JCMEC support. This will ensure that appropriate Service component resources will be allocated.

a. **Organization.** The Foreign Materiel Program managed by the DIA is the focal point for forming a JCMEC to conduct exploitation of CEE. A JCMEC is composed of Foreign Materiel Program personnel from the Service intelligence organizations and explosive ordnance disposal teams combined with the Army's 203rd Technical Intelligence (TECHINT) Battalion. It is activated during periods of joint force deployments, deployed to the AOR, and normally assigned to the supported combatant commander. DIA supplies LNOs at the theater level from which the J-2 exercises staff responsibility over all matters pertaining to CEE, including prioritizing requirements, TECHINT reporting, and coordinating with the J-3 and J-4. The J-2 also evaluates the mission and situation and determines the potential for capturing adversary materiel. These factors determine the size and composition of the JCMEC.

b. **Responsibilities.** The combatant command approves establishment of theater collection points recommended by the J-2 and sets the priority for the recovery and movement of CEE to those collection points and CONUS. The subordinate joint force and subordinate commands provide access to CEE collection points to JCMEC personnel and other supporting specialists. These personnel then evacuate CEE deemed to be valuable for intelligence or other DOD requirements. The exploitation of CEE below Army division and separate brigade, Marine Corps expeditionary force command element, and Navy and Air Force component levels is limited. Units below these levels are responsible for recovering adversary materiel and reporting its capture. Medical equipment and materiel should be exploited in the same manner as other CEE, except that cooperation and collaboration with local medical units should be established

using Geneva Convention guidelines. Suspected WMD or production equipment require special handling and must be rendered safe prior to removal to the rear area for exploitation by the JCMEC and national intelligence agencies. The local unit commander must coordinate with the JCMEC or other appropriate supporting organizations to secure the items and transport them to specially designated areas for release to technical escort personnel. Normally, a Service component commander or the JFLCC (if designated) establishes the JCMEC facility and provides or coordinates all necessary logistics, communications, siting, and transportation support for that center.

3. Joint Document Exploitation Center

Document exploitation, like equipment exploitation, is both a combatant command and national requirement. Generally, documents may be moved much more easily than CEE and will contain information on a large range of topics. Captured documents provide information on adversary intentions and planning (including deception); locations; dispositions; tactics; communications; logistics; morale; intelligence requirements and assessments; propaganda efforts aimed at friendly forces, adversary forces, and the civil populace; and equipment use, status, and operation. The category of "captured documents" includes all media capable of storing fixed information. This includes, but is not limited to paper, computer storage material, navigation devises capable of storing waypoints and other data, and other forms of stored textual and graphic information. Captured adversary documents and media files are considered unclassified unless they originated in the US and/or an allied nation, and are marked as classified. Combatant commands or subordinate joint forces requiring a JDEC should notify the NMJIC through command channels, requesting JDEC operations support. The DOD focal point for forming a JDEC is the DIA Directorate of Human Intelligence, Office of Document and Media Operations (DIA/DHX).

a. **Organization.** The JDEC should be centralized, staffed, and equipped to be able to dispatch JDEC teams to lucrative targets (e.g., adversary field staff or command locations, vehicles, airfields, or other facilities) as soon after capture as possible, or with maneuver units when such targets are anticipated. As with the JCMEC, it is activated during periods of joint force deployments, deployed to the AOR, and normally assigned to the combatant commander. The subordinate joint force J-2 exercises staff responsibility over all matters pertaining to document exploitation, including prioritizing requirements, intelligence reporting, changes to the JTMD to facilitate expansion of the JDEC mission, and coordinating with the subordinate joint force J-3 and J-4. The J-2 also evaluates the mission and situation and determines the potential for capturing adversary documents. These factors determine the size and composition of the JDEC.

b. **Responsibilities.** DIA/DHX will be prepared to deploy trained personnel and appropriate equipment to an area of conflict in order to establish an initial JDEC capability in support of operating forces. The standup phase for the JDEC is critical and its limited duration will be mutually agreed upon by DIA and the combatant commands. DIA/DHX provides JDEC CONOPS, standard operating procedures, organic mission-required ground transportation assets, and specialized mission equipment. DIA/DHX makes recommendations to combatant commands to identify and include sufficient JTMD billets to sustain document exploitations in their respective regions.

The combatant command approves priority for the recovery and movement of documents to theater collection points and CONUS as recommended by the J-2. However, the decision to move documents outside the theater of operation and/or CONUS is made by JCS. The subordinate joint force and subordinate commands provide access to captured documents to JDEC personnel and other supporting specialists. These personnel evacuate documents deemed to be valuable for intelligence or other DOD requirements. Document exploitation capabilities exist at the Army corps, Army light infantry division, and in the command element of the Marine air-ground task force, with the organic capabilities of the Navy and Air Force being more limited. Units below these levels are responsible for recovering adversary documents and reporting their capture. Normally, a Service component commander or the JFLCC, if designated, establishes the JDEC facility and provides or coordinates all necessary JDEC personnel, logistics, communications, siting, and transportation support. JDECs are manned and equipped to receive, triage, perform translation, and prioritize handling of documents and media information collected by operating forces. The JDEC disseminates information via spot reports to combatant commands and via intelligence information reports to the national IC. Exploited documents are then sent to NGIC to be uploaded into the National Harmony database.

4. Joint Interrogation and Debriefing Center

The JFC normally tasks the Army component commander to establish, secure, and maintain an EPW camp system. Under some circumstances, particularly during MOOTW, the JFC may designate another component commander to be responsible for the EPW camp system. The subordinate joint force J-2 establishes a JIDC for follow-on exploitation. The establishment (when, where, and how) of the JIDC is highly situation dependent, with the main factors being the geographic nature of the JOA, the type and pace of military operations, the camp structure, and the number and type of the sources. The JIDC may be a central site where appropriate EPW are segregated for interrogation, or it may be more of a clearinghouse operation for dispatch of interrogators or debriefers to other locations.

a. **Organization.** The JIDC interrogation and debriefing activities are managed by the subordinate joint force HUMINT staff section or HOC. The HOC will coordinate with the TFCICA within the J-2X for CI augmentation for exploitation of those personnel of CI interest, such as civil and/or military leadership, intelligence or political officers and terrorists. The cadre for the JIDC is provided by deployed DHS personnel, with augmentation as required by component TIARA and CI personnel. The HUMINT appendix of Annex B (Intelligence) to the OPLAN or CONPLAN contains JIDC planning considerations.

b. **Responsibilities.** Service component interrogators collect tactical intelligence from EPWs and ECs based on joint force J-2 criteria. EPWs (i.e., senior level EPWs) and ECs are screened by the components; those of further intelligence potential are identified and processed for follow-on interrogation and debriefing by the JIDC to satisfy theater strategic and operational requirements. In addition to EPW and ECs, the JIDC may also interrogate civilian detainees, and debrief refugees as well as other nonprisoner sources for operational and strategic information. The JIDC may identify individuals as possessing intelligence of national strategic significance; these persons may be relocated to a strategic exploitation center for longer-term interrogation.

5. Long-Term Joint Interrogation Operations

Joint interrogation operations (JIO) extend beyond the exploitation efforts conducted in theater and fulfill strategic intelligence requirements. The long-term JIO exploitation and adjudication of ECs rely heavily on information from the three exploitation centers previously profiled in this Appendix. JIO efforts against ECs normally will be conducted at a long-term detention facility external to the theater interrogation centers. JIO will be conducted in a joint or interagency environment.

a. **Organization.** US Naval Base, Guantanamo Bay, Cuba, currently serves as the external JIO facility for the exploitation of ECs from all combatant commands. All detainee operations in Guantanamo are controlled by Joint Task Force-Guantanamo (JTF-GTMO), which reports directly to the Commander, United States Southern Command. Within JTF-GTMO, JIO interrogations activities are managed by a joint interagency element known as the Joint Interrogation Group (JIG). The JIG works in concert with the detention mission, an effort managed by the joint detention operations group (JDOG). **It is imperative that the detention mission is conducted in a manner that supports interrogation efforts in the long-term exploitation facility.** The JIG and the JDOG should constantly synchronize their efforts. The JIG is managed by an element from the DIA DHS and augmented by all the Services, selected contractors, and interagency organizations.

b. **Responsibilities.** The Secretary of Defense or designee establishes policies regarding which ECs will be sent to the long-term detention facility. Policies also will be established by OSD regarding the specific conduct of JIO, the policies for foreign visits, guidelines for detainee release and transfer, and other issues, as appropriate. The combatant commander typically establishes a JTF to run the long-term detention facility where JIO takes place (for example JTF-GTMO). The JTF commander is responsible for both the detention and interrogation missions at the long-term detention facility. The JTF commander will establish detailed procedures for JIO as well as for all aspects of the detainee operations mission. The JTF will be prepared to deploy mobile detainee review and screening teams when directed. The JIG director will supervise and plan the conduct of JIO at the long-term detention facility. The Services, USJFCOM, and the participating interagency organizations will provide personnel to staff the JTF IAW the approved joint manning document. Personnel so assigned should receive focused, predeployment training that emphasizes the relationship between tactical interrogations and strategic debriefing, to include the operational coordination required within an interrogation "Tiger Team."

Intentionally Blank

APPENDIX H
INTELLIGENCE OPERATIONS EXECUTION RESPONSIBILITIES

The responsibilities for the Joint Staff J-2, combatant command J-2, subordinate joint force J-2, subordinate joint force components and the Military Services in the execution of various intelligence activities are depicted in Figures H-1 through H-7.

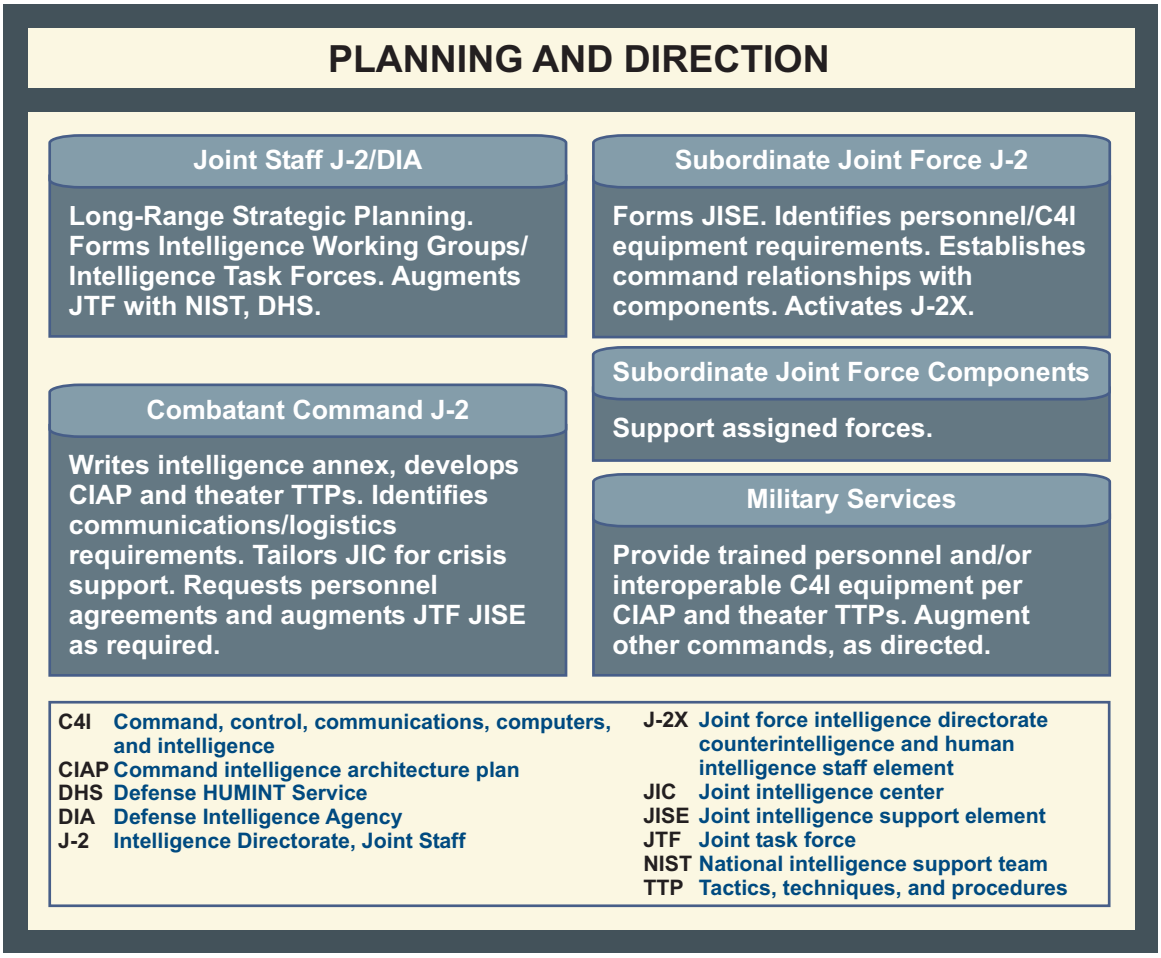


Figure H-1. Planning and Direction

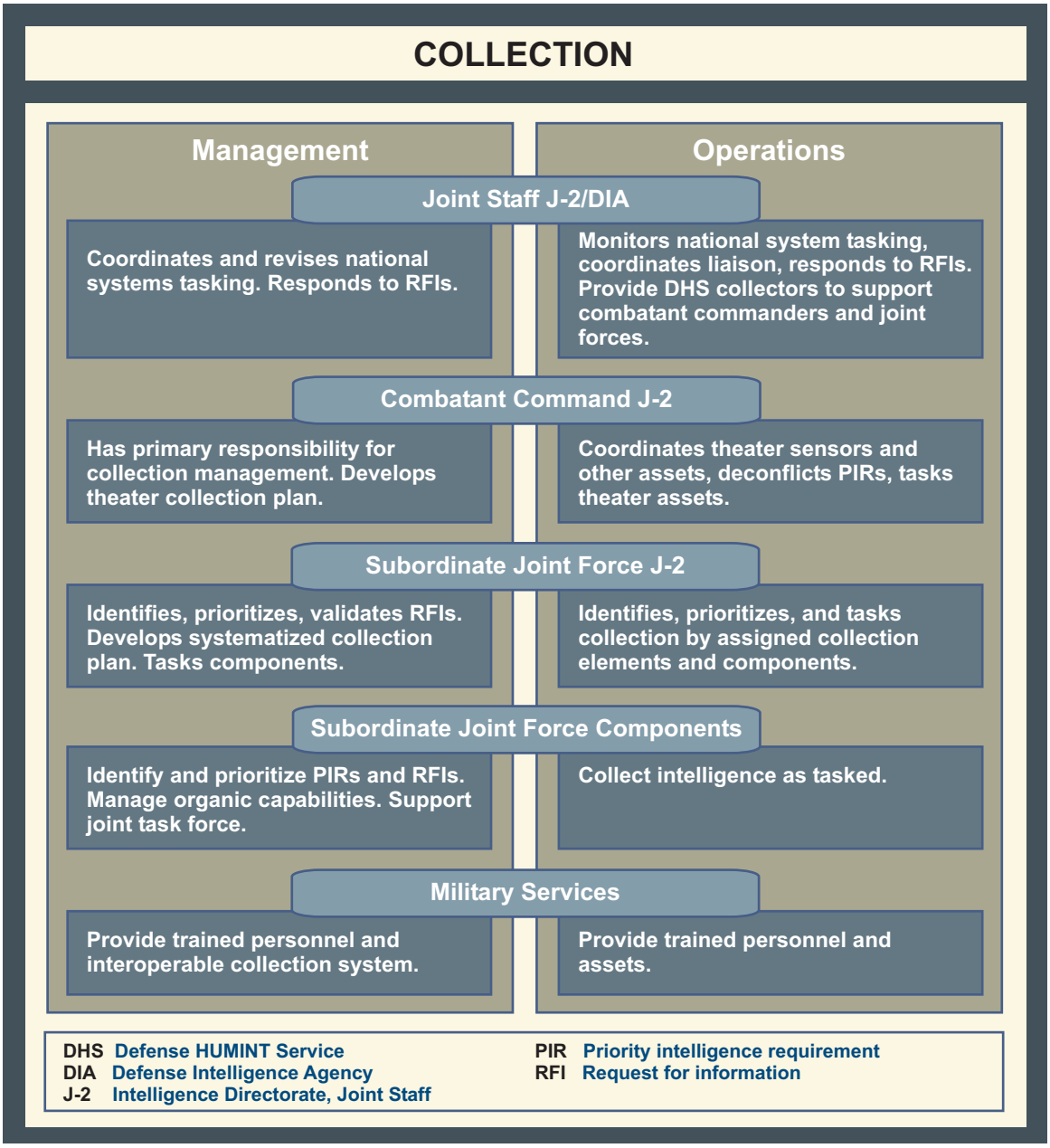


Figure H-2. Collection

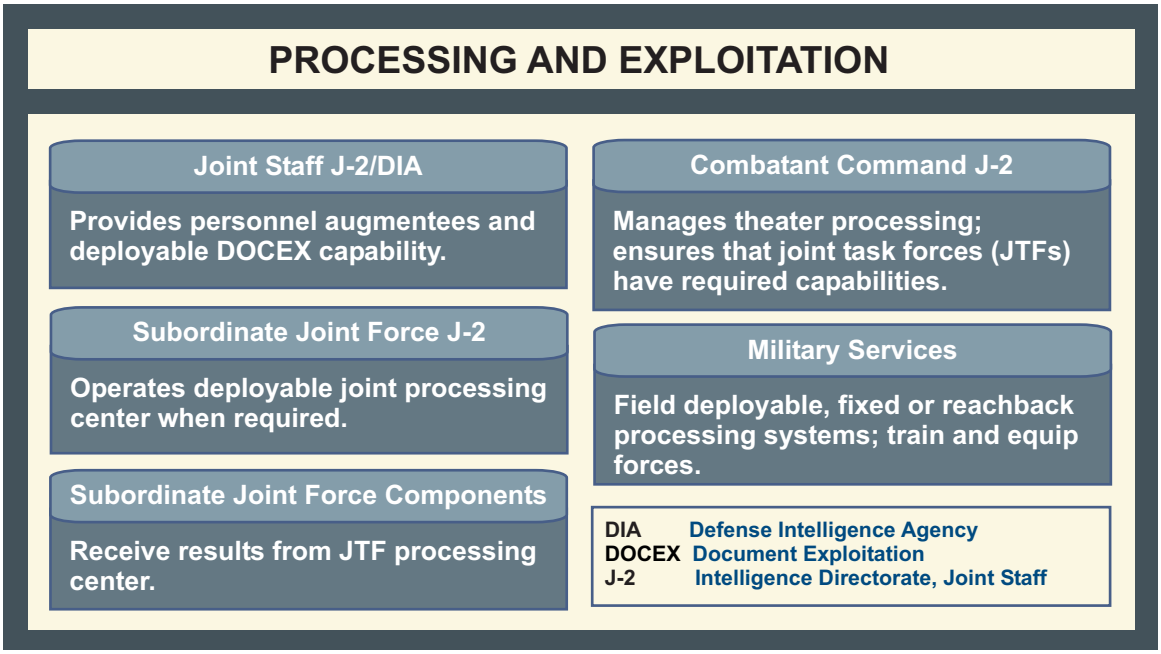


Figure H-3. Processing and Exploitation

ANALYSIS AND PRODUCTION - PART 1

	Joint Staff J-2/DIA	Combatant Command J-2
Indications and Warning (I&W)	Principal agent worldwide; theater backup	Theater expert; operates I&W center
Current Intelligence	Department of Defense focal point for fused all-source analysis and reporting	Authoritative theater estimates; maintains databases
General Military Intelligence	Intelligence communications. All-source assessments. Manages Defense Intelligence Agency (DIA) distribution process (DPP)	Theater assessments, maintains databases, DPP participant
Target Intelligence	Focal point for target intelligence support to President, Secretary of Defense, Chairman of the Joint Chiefs of Staff, Joint Staff, and combatant commands. Coordinates national-level target intel support for Chairman of the Joint Chiefs of Staff/Command Deliberate Planning/Crisis Ops. Directs national-level bomb damage assessment. Responsible for target intelligence policy, standards, procedures, requirements, and automation	Develops, validates, nominates, and prioritizes theater targets. Directs theater battle damage assessment process
Science and Technology	Manages Department of Defense scientific and technical centers; coordinates scientific and technical intelligence requirements with combatant commander; provides joint captured materiel exploitation center personnel augmentees	Validates national technical intelligence requirements; coordinates movement of captured materiel

Figure H-4. Analysis and Production — Part 1

ANALYSIS AND PRODUCTION - PART 2

	Subordinate Joint Force J-2	Subordinate Joint Force Components	Military Services
Indications and Warning (I&W)	I&W consumer; monitors and reports	I&W consumers; monitor and report	I&W consumers; train personnel in defense I&W systems
Current Intelligence	Mission-specific intelligence; prioritizes requests for intelligence	Customers; provide request for information to joint task force (JTF) joint intelligence support element	Customers; augment National Military Joint Intelligence Center
General Military Intelligence	User of general military intelligence; tailors to JTF focus	Intelligence Production Schedule	Distributed production program participants; augment joint intelligence center production
Target Intelligence	Develops, validates, nominates, and prioritizes theater targets. Administers theater battle damage assessment process.	Develops, validates, nominates, and prioritizes component-related targets. Reports mission battle damage assessment.	Train target personnel; provide specialized functional products
Science and Technology	Executes technical intelligence mission in the operational area	Provide technical intelligence collection requirements to forces	Manage scientific and technical centers; provide personnel augmentees to JTF; provide specialized analysis

Figure H-5. Analysis and Production — Part 2

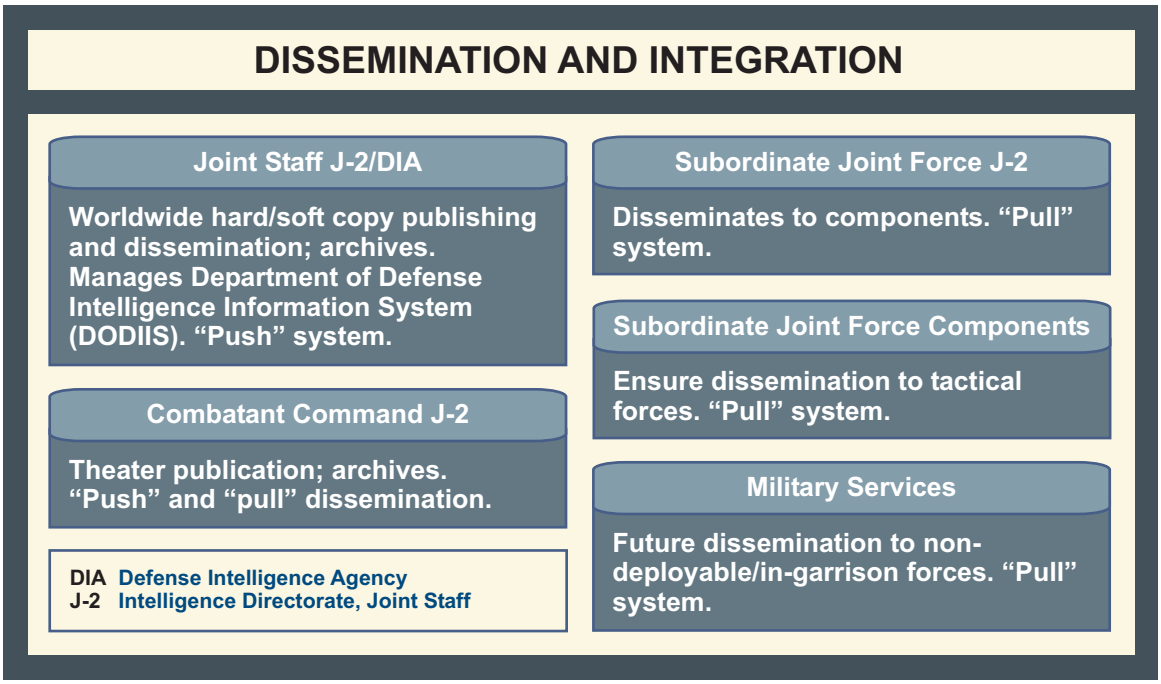


Figure H-6. Dissemination and Integration

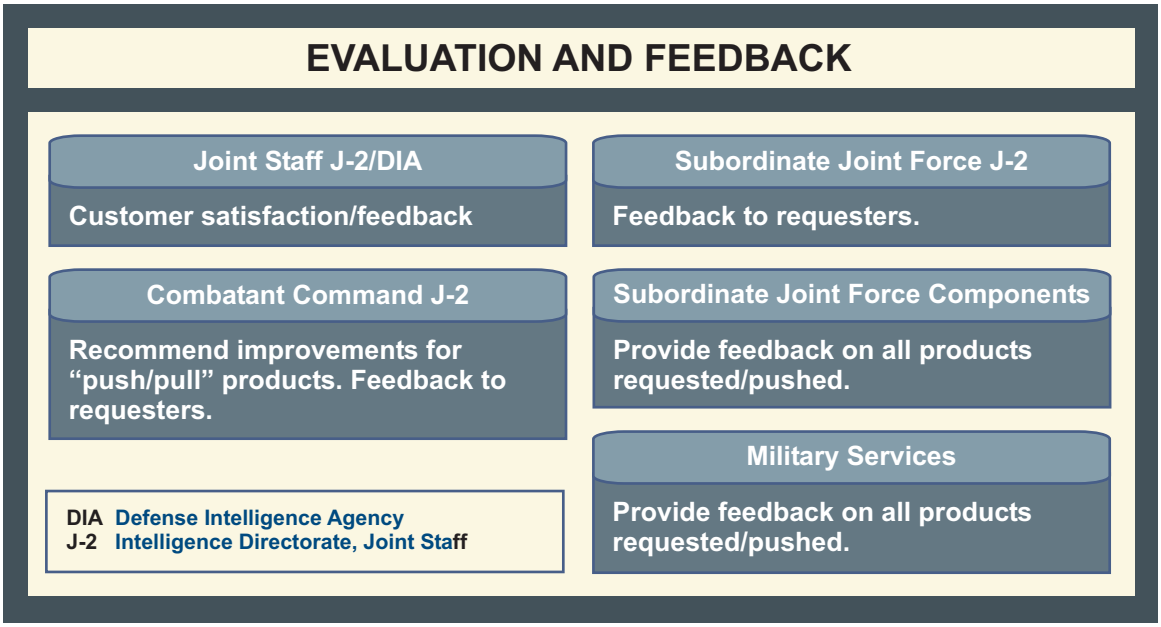


Figure H-7. Evaluation and Feedback

APPENDIX J
REFERENCES

The development of JP 2-01 is based upon the following primary references.

1. National Security Act of 1947, as amended.

2. Title 10, United States Code Armed Forces, as amended.

3. Goldwater-Nichols Department of Defense Reorganization Act of 1986.

4. *The National Security Strategy of the United States.*

5. *National Strategy to Combat Weapons of Mass Destruction.*

6. *National Strategy for Homeland Security.*

7. *National Strategy for Combating Terrorism.*

8. Executive Order (EO) 12333, *United States Intelligence Activities*.

9. EO 12958, *Classified National Security Information*.

10. JP 1, *Joint Warfare of the Armed Forces of the United States*.

11. JP 0-2, *Unified Action Armed Forces (UNAAF)*.

12. JP 1-0, *Doctrine for Personnel Support to Joint Operations*.

13. JP 1-01, *Joint Doctrine Development System*.

14. JP 1-02, *DOD Dictionary of Military and Associated Terms*.

15. JP 2-0, *Doctrine for Intelligence Support to Joint Operations*.

16. JP 2-01.1, *Joint Tactics, Techniques, and Procedures for Intelligence Support to Targeting*.

17. JP 2-01.2, *Joint Doctrine, Tactics, Techniques, and Procedures for Counterintelligence Support to Operations*.

18. JP 2-01.3, *Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace*.

19. JP 2-03, *Joint Tactics, Techniques, and Procedures for Geospatial Information and Services Support to Joint Operations*.

20. JP 3-0, *Doctrine for Joint Operations*.

21. JP 3-05, *Doctrine for Joint Special Operations.*

22. JP 3-11, *Joint Doctrine for Operations in Nuclear, Biological, and Chemical Environments.*

23. JP 3-40, *Joint Doctrine for Combating Weapons of Mass Destruction.*

24. JP 3-50, *Joint Doctrine for Personnel Recovery.*

25. JP 3-53, *Doctrine for Joint Psychological Operations.*

26. JP 3-54, *Joint Doctrine for Operations Security.*

27. JP 5-0, *Doctrine for Planning Joint Operations*.

28. JP 5-00.2, *Joint Task Force Planning Guidance and Procedures*.

29. JP 6-0, *Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations*.

30. NDP-1, *National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations* (Short Title: *National Defense Policy*).

31. DODD C-5105.32, *Defense Attache System* (U).

32. DODD 5105.67, *Counterintelligence Field Activity.*

33. DODD 5200.2-R, *DOD Personnel Security Program*.

34. DODD 5200.27, *Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense*.

35. DODD 5205.1, *Acquisition and Reporting of Information Relating to National Security*.

36. DODD S-5210.36, *Provision of DOD Sensitive Support to DOD Components and Other Departments and Agencies of the US Government*.

37. DODD 5230-11, *Disclosure of Classified Military Information to Foreign Governments and International Organizations*.

38. DODD 5240.1, *DOD Intelligence Activities*.

39. DODD 5240.2, *DOD Counterintelligence.*

40. DODD 5240.10, *Counterintelligence Support to the Combatant Commands and the Defense Agencies.*

41. DOD-0000-151-YR, *DOD Intelligence Production Program*.

42. DOD-0000-151A-YR, *DOD Intelligence Production Program: Production Responsibilities*.

43. DOD-0000-151B-YR, *DOD Intelligence Production Program: Production Priorities*.

44. DOD-0000-151C-YR, *DOD Intelligence Production Program: Production Procedures*.

45. DOD S-5105.21-M-1, *Sensitive Compartmented Information Administrative Security (SCIFs) Manual*.

46. DCID 1/21, *Physical Security Standards for SCIFs*.

47. DCID 5/1, *Espionage and Counterintelligence Activities Abroad*.

48. DCID 6/6, *Security Controls on the Dissemination of Intelligence Information*.

49. DCID 6/7, *Intelligence Disclosure Policy*.

50. DCS-2600-5345-92, *DIA Guide to Foreign Disclosure*.

51. DIAM 58-5, *Imagery Requirements*.

52. DIAM 58-8, *Measurement and Signature Intelligence (MASINT) User's Guide*.

53. DIAM 58-11, *DOD Human Intelligence (HUMINT) Policies and Procedures*.

54. DIAM 58-12, *DOD Human Intelligence (HUMINT) Management System*.

55. DIAM 58-17, *Defense Signals Intelligence (SIGINT) Requirements Manual*.

56. DIA, *The Roadmap to the 21st Century Production Environment*.

57. DIA, *Joint Intelligence Virtual Architecture Strategic Plan and Implementation Plan*.

58. DISA, *Defense Information Infrastructure Common Operating Environment*.

59. Marine Corps Manual-15-94, *Memorandum of Agreement Concerning CIA Support to US Military Forces*.

60. CJCSI 1301.01A, *Policy and Procedures to Assign Individuals to Meet Combatant Command Mission Related Temporary Duty Requirements*.

61. CJCSI 3151.01, *Global Command and Control System Common Operational Picture Reporting Requirements*.

62. CJCSI 3210.01A, *Joint Information Operations Policy*.

63. CJCSI 3250 (Series), *Policy Guidance for Sensitive Airborne and Maritime Surface Reconnaissance Operations*.

64. CJCSI 3270.01a, *Personnel Recovery within the Department of Defense.*

65. CJCSI 5221.01A, *Delegation of Authority to Commanders of Combatant Commands to Disclose Classified Military Information to Foreign Governments and International Organizations*.

66. CJCSI 6110.01, *CJCS-Controlled Tactical Communications Assets*.

67. CJCSI 6212.01B, *Interoperability and Supportability of National Security Systems, and Information Technology Systems*.

68. CJCSM 3122.02A, *Crisis Action Time-Phased Force and Deployment Data Development and Deployment Execution, Volume II*.

69. CJCSM 3122.03A, *Joint Operation Planning and Execution System, Vol II: (Planning Formats and Guidance)*.

70. CJCSM 3122.04A, *Joint Operation Planning and Execution System, Vol II: (Supplemental Planning Formats and Guidance)*.

71. NRO/OSO, *Joint Tactical Exploitation of National Systems (JTENS) Manual*.

72. NGA, *Imagery Policy Series (IPS)*.

73. Director Central Intelligence National SIGINT Committee, *Handbook of the National SIGINT Requirements System*.

74. IPSG/INCA-133, *Communications Handbook for Intelligence Planners*.

75. USIS Directive 2-0, *Imagery Processing, Exploitation, and Delivery Policy*.

76. Public Law 585, *Atomic Energy Act of 1954*, as amended.

77. Joint Staff J-8, Report to Congress: *Kosovo/Operation Allied Force After-Action Report*.

APPENDIX K
ADMINISTRATIVE INSTRUCTIONS

1. User Comments

Users in the field are highly encouraged to submit comments on this publication to: Commander, United States Joint Forces Command, Joint Warfighting Center Code JW100, 116 Lake View Parkway, Suffolk, VA 23435-2697. These comments should address content (accuracy, usefulness, consistency, and organization), writing, and appearance.

2. Authorship

The lead agent and the Joint Staff doctrine sponsor for this publication is the Director for Intelligence (J-2).

3. Supersession

This publication supersedes JP 2-01, 20 November 1996, *Joint Intelligence Support to Military Operations,* and JP 2-02, 28 September 1998, *National Intelligence Support to Joint Operations*.

4. Change Recommendations

a. Recommendations for urgent changes to this publication should be submitted:

TO: JOINT STAFF WASHINGTON DC//J2-J2P/J7-JEDD//
INFO: USCDRJFCOM SUFFOLK VA//JW100

Routine changes should be submitted to the Director for Operational Plans and Joint Force Development (J-7), JEDD, 7000 Joint Staff Pentagon, Washington, DC 20318-7000, with info copies to the USJFCOM JWFC.

b. When a Joint Staff directorate submits a proposal to the Chairman of the Joint Chiefs of Staff that would change source document information reflected in this publication, that directorate will include a proposed change to this publication as an enclosure to its proposal. The Military Services and other organizations are requested to notify the Director, J-7, Joint Staff, when changes to source documents reflected in this publication are initiated.

c. Record of Changes:

CHANGE NUMBER	COPY NUMBER	DATE OF CHANGE	DATE ENTERED	POSTED BY	REMARKS

5. Distribution

a. Additional copies of this publication can be obtained through Service publication centers listed below (initial contact) or the USJFCOM JWFC in the event that the joint publication is not available from the Service.

b. Only approved joint publications and joint test publications are releasable outside the combatant commands, Services, and Joint Staff. Release of any classified joint publication to foreign governments or foreign nationals must be requested through the local embassy (Defense Attaché Office) to DIA Foreign Liaison Office, PO-FL, Room 1E811, 7400 Defense Pentagon, Washington, DC 20301-7400.

c. Additional copies should be obtained from the Military Service assigned administrative support responsibility by DOD Directive 5100.3, 15 November 1999, *Support of the Headquarters of Unified, Specified, and Subordinate Joint Commands*.

Army:	US Army AG Publication Center SL 1655 Woodson Road Attn: Joint Publications St. Louis, MO 63114-6181
Air Force:	Air Force Publications Distribution Center 2800 Eastern Boulevard Baltimore, MD 21220-2896
Navy:	CO, Naval Inventory Control Point 700 Robbins Avenue Bldg 1, Customer Service Philadelphia, PA 19111-5099
Marine Corps:	Commander (Attn: Publications) 814 Radford Blvd, Suite 20321 Albany, GA 31704-0321
Coast Guard:	Commandant Coast Guard (G-OPD), US Coast Guard 2100 2nd Street, SW Washington, DC 20593-0001
	Commander USJFCOM JWFC Code JW2102 Doctrine Division (Publication Distribution) 116 Lake View Parkway Suffolk, VA 23435-2697

d. Local reproduction is authorized and access to unclassified publications is unrestricted. However, access to and reproduction authorization for classified joint publications must be in accordance with DOD Regulation 5200.1-R, *Information Security Program*.

Intentionally Blank

GLOSSARY
PART I — ABBREVIATIONS AND ACRONYMS

AAA	antiaircraft artillery
ACIC	Army Counterintelligence Center
AFB	Air Force base
AFIWC	Air Force Information Warfare Center
AFMIC	Armed Forces Medical Intelligence Center
AFOSI	Air Force Office of Special Investigations
AF/XOI	Air Force Director of Intelligence, Surveillance, and Reconnaissance
AIA	Air Intelligence Agency
AIRBAT	Airborne Intelligence, Surveillance, and Reconnaissance Requirements-Based Allocation Tool
AOR	area of responsibility
ARFOR	Army forces
BDA	battle damage assessment
BW	biological warfare
C2	command and control
C2W	command and control warfare
C3	command, control, and communications
C4	command, control, communications, and computers
C4I	command, control, communications, computers, and intelligence
CA	combat assessment
CAP	crisis action planning
CCIR	commander's critical information requirement
CCP	consolidated cryptologic program
CD-ROM	compact disc read-only memory
CDRUSSTRATCOM	Commander, United States Strategic Command
CE	counterespionage
CEE	captured enemy equipment
CENTRIXS	Combined Enterprise Regional Information Exchange System
CGIS	US Coast Guard Investigative Service
CI	counterintelligence
CIA	Central Intelligence Agency
CIAP	Central Intelligence Agency program
CIFA	Counterintelligence Field Activity
CISO	counterintelligence support officer
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff instruction
CJCSM	Chairman of the Joint Chiefs of Staff manual
C-JWICS	Containerized Joint Worldwide Intelligence Communications System

CMA	collection management authority
CMMA	collection management mission application
CMS	community management staff
CNO	Chief of Naval Operations
CNSG	Commander, Naval Security Group
COA	course of action
COG	center of gravity
COLISEUM	community on-line intelligence system for end-users and managers
COM	collection operations management
COMINT	communications intelligence
COMSEC	communications security
CONOPS	concept of operations
CONPLAN	operation plan in concept format
CONUS	continental United States
COOP	continuity of operations
COP	common operational picture
COT	crisis operations team
CPG	Contingency Planning Guidance
CRM	collection requirements management
CS	critical source
CSG	cryptologic services group
CSS	central security service
D&D	denial and deception
DA	Directorate for Administration (DIA)
DAC	Defense Intelligence Agency (DIA) counterintelligence and security activity
DCCC	defense collection coordination center
DCGS	Distributed Common Ground/Surface System
DCI	Director of Central Intelligence
DCID	Director of Central Intelligence directive
DCS	deputy chief of staff
DDCI/CM	Deputy Director of Central Intelligence for Community Management
DDMS	Deputy Director for Military Support
DEA	Drug Enforcement Administration
DEPORD	deployment order
DGIAP	Defense General Intelligence and Applications Program
DH	Directorate for Human Intelligence (DIA)
DHS	Defense Human Intelligence (HUMINT) Service
DI	Defense Intelligence Agency (DIA) Directorate for Analysis
DIA	Defense Intelligence Agency
DIAC	Defense Intelligence Analysis Center
DIA/DHX	Defense Intelligence Agency, Directorate of Human Intelligence,

	Office of Document and Media Operations
DIAM	Defense Intelligence Agency manual
DIDS	Defense Intelligence Dissemination System
DIEB	Defense Intelligence Executive Board
DIRINT	Director of Intelligence
DIRNSA	Director, National Security Agency
DISA	Defense Information Systems Agency
DISO	defense intelligence support office
DMS	defense message system
DNI	Director of Naval Intelligence
DOCEX	document exploitation
DOD	Department of Defense
DODD	Department of Defense directive
DODIIS	Department of Defense Intelligence Information System
DODIPC	Department of Defense intelligence production community
DODIPP	Department of Defense Intelligence Production Program
DOE	Department of Energy
DOS	Department of State
DPM	dissemination program manager
DS	Directorate for Information Systems and Services (DIA)
DT	Directorate for MASINT and Technical Collection (DIA)
DTRA	Defense Threat Reduction Agency
DX	Directorate for External Relations (DIA)
EAC	echelons above corps
EC	enemy combatant
EEI	essential element of information
ELINT	electronic intelligence
EO	executive order
EPW	enemy prisoner of war
EW	electronic warfare
1st IOC	1st Information Operations Command (Land)
FAX	facsimile
FBI	Federal Bureau of Investigation
FBIS	Foreign Broadcast Information Service
FIS	Foreign Intelligence Service
FISINT	foreign instrumentation signals intelligence
G-2	Army or Marine Corps component intelligence staff officer (Army Division or higher staff, Marine Corps brigade or higher staff)
G-3	Army or Marine Corps component operations staff officer (Army division or higher staff, Marine Corps brigade or higher staff)

GBS	Global Broadcast Service
GCCS	Global Command and Control System
GCCS-I3	Global Command and Control System Integrated Imagery and Intelligence
GCI	ground control intercept
GDIP	General Defense Intelligence Program
GEOINT	geospatial intelligence
GI&S	geospatial information and services
GIG	Global Information Grid
GMFP	global military force policy
GMI	general military intelligence
HMMWV	high mobility multipurpose wheeled vehicle
HNS	host-nation support
HOC	human intelligence operations cell
HQ	headquarters
HSE	human intelligence (HUMINT) support element
HUMINT	human intelligence
I&W	indications and warning
IA	information assurance
IAIP	Information Analysis and Infrastructure Protection
IAW	in accordance with
IC	intelligence community
ICC	Intelligence Coordination Center
ICDC	Intelligence Community Deputies Committee
ICPC	Intelligence Community Principals Committee
IEW	intelligence and electronic warfare
IMINT	imagery intelligence
INMARSAT	international maritime satellite
INR	Bureau of Intelligence and Research, Department of State
INSCOM	United States Army Intelligence and Security Command
IO	information operations
IP	internet protocol
IPB	intelligence preparation of the battlespace
IPL	imagery product library
ISR	intelligence, surveillance, and reconnaissance
ISSG	Intelligence Senior Steering Group
IT	information technology
ITF	intelligence task force (DIA)
IW	information warfare
IWG	intelligence working group
J-1	manpower and personnel directorate of a joint staff
J-2	intelligence directorate of a joint staff

J-2A	deputy directorate for administration of a joint staff
J-2J	deputy directorate for support of a joint staff
J-2M	deputy directorate for crisis management of a joint staff
J-2O	deputy directorate for crisis operations of a joint staff
J-2P	deputy directorate for assessment, doctrine, requirements, and capabilities of a joint staff
J-2T	deputy directorate for targets of a joint staff
J-2T-1	joint staff target operations division
J-2T-2	Target Plans Division
J-2X	joint force J-2 CI/HUMINT staff element
J-3	operations directorate of a joint staff
J-4	logistics directorate of a joint staff
J-5	plans directorate of a joint staff
J-6	command, control, communications, and computer systems directorate of a joint staff
J-8	force structure, resource, and assessment directorate of a joint staff
JAC	joint analysis center
JCE	Joint Intelligence Virtual Architecture (JIVA) Collaborative Environment
JCMA	joint communications security monitor activity
JCMB	joint collection management board
JCMEC	joint captured materiel exploitation center
JCS	Joint Chiefs of Staff
JCSE	joint communications support element
JDEC	joint document exploitation center
JDISS	joint deployable intelligence support system
JDOG	joint detention operations group
JFC	joint force commander
JFLCC	joint force land component commander
JIC	joint intelligence center
JIDC	joint interrogation and debriefing center
JIG	joint interrogation group
JIO	joint interrogation operations
JIOC	joint information operations center
JIPB	joint intelligence preparation of the battlespace
JIPCL	joint integrated prioritized collection list
JISE	joint intelligence support element
JITF-CT	Joint Intelligence Task Force – Combating Terrorism
JIVA	Joint Intelligence Virtual Architecture
JMICS	Joint Worldwide Intelligence Communications System (JWICS) mobile integrated communications system
JMIP	joint military intelligence program
JMITC	Joint Military Intelligence Training Center
JOA	joint operations area

JOPES	Joint Operation Planning and Execution System
JP	joint publication
JROC	Joint Requirements Oversight Council
JSCP	Joint Strategic Capabilities Plan
JSST	joint space support team
JTF	joint task force
JTF-GTMO	Joint Task Force-Guantanamo
JTMD	joint table of mobilization and distribution
JWAC	joint warfare analysis center
JWICS	Joint Worldwide Intelligence Communications System
LAN	local area network
LNO	liaison officer
LOCE	Linked Operations-Intelligence Centers Europe
LOC	line of communications
LOS	line of sight
MASINT	measurement and signature intelligence
MASLO	measurement and signature intelligence (MASINT) liaison officer
MCIA	Marine Corps Intelligence Activity
METOC	meteorological and oceanographic
MI	military intelligence
MIB	Military Intelligence Board
MIDB	modernized integrated database
MNFC	multinational force commander
MOA	memorandum of agreement
MOCC	measurement and signature intelligence (MASINT) operations coordination center
MOOTW	military operations other than war
MRS	measurement and signature intelligence (MASINT) requirements system
MSIC	Missile and Space Intelligence Center
MTAC	Multiple Threat Alert Center
NASIC	National Air and Space Intelligence Center
NATO	North Atlantic Treaty Organization
NCIS	Naval Criminal Investigative Service
NCR	National Security Agency/Central Security Service representative
NCRDEF	national cryptologic representative defense
NDP	national disclosure policy
NDPC	National Disclosure Policy Committee
NFIB	National Foreign Intelligence Board
NFIP	National Foreign Intelligence Program
NGA	National Geospatial-Intelligence Agency

NGIC	National Ground Intelligence Center
NGP	National Geospatial-Intelligence Agency Program
NIC	National Intelligence Council
NIPRNET	Nonsecure Internet Protocol Router Network
NIST	national intelligence support team
NIWA	naval information warfare activity
NMCC	National Military Command Center
NMIC	National Maritime Intelligence Center
NMJIC	National Military Joint Intelligence Center
NRC	National Response Center
NRO	National Reconnaissance Office
NRT	near real time
NRTD	near-real-time dissemination
NSA	National Security Agency
NSC	National Security Council
NSGI	National System for Geospatial Intelligence
NSOC	National Security Operations Center
NST	National Geospatial-Intelligence Agency support team
NSTS	National Secure Telephone System
NTBC	National Military Joint Intelligence Center Targeting and Battle Damage Assessment Cell
OB	order of battle
OCONUS	outside the continental United States
OICC	operational intelligence coordination center
OMA	Office of Military Affairs (CIA)
ONDCP	Office of National Drug Control Policy
ONI	Office of Naval Intelligence
OPCON	operational control
OPLAN	operation plan
OPORD	operation order
OPSEC	operations security
OSD	Office of the Secretary of Defense
OSINT	open-source intelligence
OSIS	open-source information system
PFIAB	President's Foreign Intelligence Advisory Board
PGM	precision-guided munition
PIR	priority intelligence requirement
PMGM	program manager's guidance memorandum
POC	point of contact
POL	petroleum, oils, and lubricants
PR	production requirement
PSYOP	psychological operations

QRT	quick reaction team
RFI	request for information
RPPO	Requirements, Plans, and Policy Office
RSOC	regional signals intelligence (SIGINT) operations center
S&T	scientific and technical
S&TI	scientific and technical intelligence
SAM	surface-to-air missile
SATCOM	satellite communications
SCE	Service cryptologic element
SCI	sensitive compartmented information
SCIF	sensitive compartmented information facility
SecDef	Secretary of Defense
SIGINT	signals intelligence
SII	statement of intelligence interest
SIO	senior intelligence officer
SIPRNET	SECRET Internet Protocol Router Network
SIR	specific information requirement
SOF	special operations forces
SOIC	senior officer of the Intelligence Community
SPP	shared production program
SSA	special support activity
SSM	surface-to-surface missile
SSO	special security office(r)
SST	special support team (National Security Agency)
STANAG	standardization agreement
TBM	theater ballistic missile
TECHINT	technical intelligence
TENCAP	tactical exploitation of national capabilities program
TFCICA	task force counterintelligence coordinating authority
TIARA	tactical intelligence and related activities
TIM	toxic industrial material
TPED	tasking, processing, exploitation, and dissemination
TPFDD	time-phased force and deployment data
TPFDL	time-phased force and deployment list
TSCM	technical surveillance countermeasures
TSR	theater support representative
TSWA	temporary secure working area
TTP	tactics, techniques, and procedures
UAV	unmanned aerial vehicle
UHF	ultrahigh frequency
UN	United Nations

UNOSOM	United Nations Operations in Somalia
USCG	United States Coast Guard
USCS	US cryptologic system
USD(I)	Under Secretary of Defense (Intelligence)
USEUCOM	United States European Command
USFK	United States Forces Korea
USG	United States Government
USJFCOM	United States Joint Forces Command
USSTRATCOM	United States Strategic Command
USTRANSCOM	United States Transportation Command
UW	unconventional warfare
VO	validation office
VTC	video teleconferencing
WAN	wide-area network
WMD	weapons of mass destruction

agency. In intelligence usage, an organization or individual engaged in collecting and/or processing information. Also called collection agency. (JP 1-02)

all-source intelligence. 1. Intelligence products and/or organizations and activities that incorporate all sources of information, most frequently including human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open- source data in the production of finished intelligence. 2. In intelligence collection, a phrase that indicates that in the satisfaction of intelligence requirements, all collection, processing, exploitation, and reporting systems and resources are identified for possible use and those most capable are tasked. (JP 1-02)

analysis and production. In intelligence usage, the conversion of processed information into intelligence through the integration, evaluation, analysis, and interpretation of all source data and the preparation of intelligence products in support of known or anticipated user requirements. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

battle damage assessment. The timely and accurate estimate of damage resulting from the application of military force, either lethal or nonlethal, against a predetermined objective. Battle damage assessment can be applied to the employment of all types of weapon systems (air, ground, naval, and special forces weapon systems) throughout the range of military operations. Battle damage assessment is primarily an intelligence responsibility with required inputs and coordination from the operators. Battle damage assessment is composed of physical damage assessment, functional damage assessment, and target system assessment. Also called BDA. See also combat assessment. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

battlespace. The environment, factors, and conditions that must be understood to successfully apply combat power, protect the force, or complete the mission. This includes the air, land, sea, space, and the included enemy and friendly forces; facilities; weather; terrain; the electromagnetic spectrum; and the information environment within the operational areas and areas of interest. (JP 1-02)

battlespace awareness. Knowledge and understanding of the operational area's environment, factors, and conditions, to include the status of friendly and adversary forces, neutrals and noncombatants, weather and terrain, that enables timely, relevant, comprehensive, and accurate assessments, in order to successfully apply combat power, protect the force, and/or complete the mission. (Approved for inclusion in the next edition of JP 1-02.)

collection. In intelligence usage, the acquisition of information and the provision of this information to processing elements. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

collection asset. A collection system, platform, or capability that is supporting, assigned, or attached to a particular commander. (JP 1-02)

collection management. In intelligence usage, the process of converting intelligence requirements into collection requirements, establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring results, and retasking, as required. (JP 1-02)

collection management authority. Constitutes the authority to establish, prioritize and validate theater collection requirements, establish sensor tasking guidance, and develop theater collection plans. Also called CMA. (JP 1-02)

collection manager. An individual with responsibility for the timely and efficient tasking of organic collection resources and the development of requirements for theater and national assets that could satisfy specific information needs in support of the mission. Also called CM. (JP 1-02)

collection operations management. The authoritative direction, scheduling, and control of specific collection operations and associated processing, exploitation, and reporting resources. Also called COM. (JP 1-02)

collection plan. A plan for collecting information from all available sources to meet intelligence requirements and for transforming those requirements into orders and requests to appropriate agencies. (JP 1-02)

collection planning. A continuous process that coordinates and integrates the efforts of all collection units and agencies. See also collection. (JP 1-02)

collection requirement. An established intelligence need considered in the allocation of intelligence resources to fulfill the essential elements of information and other intelligence needs of a commander. (JP 1-02)

collection requirements management. The authoritative development and control of collection, processing, exploitation, and/or reporting requirements that normally result in either the direct tasking of assets over which the collection manager has authority, or the generation of tasking requests to collection management authorities at a higher, lower, or lateral echelon to accomplish the collection mission. Also called CRM. (JP 1-02)

collection resource. A collection system, platform, or capability that is not assigned or attached to a specific unit or echelon which must be requested and coordinated through the chain of command. (JP 1-02)

combat assessment. The determination of the overall effectiveness of force employment during military operations. Combat assessment is composed of three major components: (a) battle damage assessment; (b) munitions effectiveness assessment; and (c) reattack recommendation. Also called CA. (JP 1-02)

combat intelligence. That knowledge of the enemy, weather, and geographical features required by a commander in the planning and conduct of combat operations. (JP 1-02)

command and control warfare. The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions. Command and control warfare is an application of information operations in military operations. Also called C2W. C2W is both offensive and defensive: a. C2-attack. Prevent effective C2 of adversary forces by denying information to, influencing, degrading, or destroying the adversary C2 system. b. C2-protect. Maintain effective command and control of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade, or destroy the friendly C2 system. (JP 1-02)

commander's critical information requirements. Commander's critical information requirements comprise information requirements identified by the commander as being critical in facilitating timely information management and the decision-making process that affect successful mission accomplishment. The two key subcomponents are critical friendly force information and priority intelligence requirements. Also called CCIRs. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

common operational picture. A single identical display of relevant information shared by more than one command. A common operational picture facilitates collaborative planning and assists all echelons to achieve situational awareness. Also called COP. (JP 1-02)

communications intelligence. Technical information and intelligence derived from foreign communications by other than the intended recipients. Also called COMINT. (JP 1-02)

concept of intelligence operations. A verbal or graphic statement, in broad outline, of an intelligence directorate's assumptions or intent regarding intelligence support of an operation or series of operations. The concept of intelligence operations, which complements the commander's concept of operations, is contained in the intelligence annex of operation plans. The concept of intelligence operations is designed to give an overall picture of intelligence support for joint operations. It is included primarily for additional clarity of purpose. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

counterintelligence. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign

governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. Also called CI. (JP 1-02)

counterintelligence activities. The four functions of counterintelligence: operations; investigations; collection; and analysis and production. (JP 1-02)

counterintelligence operations. Proactive activities designed to identify, exploit, neutralize, or deter foreign intelligence collection and terrorist activities directed against the Department of Defense (DOD). Operations are conducted to: manipulate, disrupt, neutralize, and/or destroy the effectiveness of foreign intelligence activities; recruit or induce defection of foreign intelligence officers and personnel; collect threat information on foreign intelligence operations, modus operandi, intelligence requirements, targeting, objectives, personalities, communications, capabilities, limitations, and vulnerabilities; provide information and operations databases to support decision makers; provide counterintelligence (CI) support to clandestine human intelligence operations; identify post, ongoing, or planned espionage; support force protection, operations other than war, and peacekeeping; acquire foreign intelligence espionage equipment for analysis and countermeasures development; develop operational data, threat data, and espionage leads for future CI operations, investigations, and projects and develop the potential of these leads to enhance DOD security overall; and support specific Chairman of the Joint Chiefs of Staff, DOD, and national plans. (JP 1-02)

counterproliferation. Those actions (e.g., detect and monitor, prepare to conduct counterproliferation operations, offensive operations, weapons of mass destruction, active defense, and passive defense) taken to defeat the threat and/or use of weapons of mass destruction against the United States, our military forces, friends, and allies. (JP 1-02)

critical intelligence. Intelligence that is crucial and requires the immediate attention of the commander. It is required to enable the commander to make decisions that will provide a timely and appropriate response to actions by the potential or actual enemy. It includes but is not limited to the following: a. strong indications of the imminent outbreak of hostilities of any type (warning of attack); b. aggression of any nature against a friendly country; c. indications or use of nuclear, biological, and chemical weapons; and d. significant events within potential enemy countries that may lead to modification of nuclear strike plans. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

database. Information that is normally structured and indexed for user access and review. Databases may exist in the form of physical files (folders, documents, etc.) or formatted automated data processing system data files. (JP 1-02)

deception. Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce the enemy to react in a manner prejudicial to the enemy's interests. (JP 1-02)

Defense Information Systems Network. Integrated network, centrally managed and configured to provide long-haul information transfer services for all Department of Defense activities. It is an information transfer utility designed to provide dedicated point-to-point, switched voice and data, imagery, and video teleconferencing services. Also called DISN. (JP 1-02)

Department of Defense Intelligence Information System. The combination of Department of Defense personnel, procedures, equipment, computer programs, and supporting communications that support the timely and comprehensive preparation and presentation of intelligence and information to military commanders and national-level decision makers. Also called DODIIS. (JP 1-02)

dissemination and integration. In intelligence usage, the delivery of intelligence to users in a suitable form and the application of the intelligence to appropriate missions, tasks, and functions. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

electronic intelligence. Technical and geolocation intelligence derived from foreign non-communications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. Also called ELINT. (JP 1-02)

enemy combatant. Any person in an armed conflict who could be properly detained under the laws and customs of war. Also called EC. (Approved for inclusion in the next edition of JP 1-02.)

essential elements of friendly information. Key questions likely to be asked by adversary officials and intelligence systems about specific friendly intentions, capabilities, and activities, so they can obtain answers critical to their operational effectiveness. Also called EEFI. (JP 1-02)

essential elements of information. The most critical information requirements regarding the adversary and the environment needed by the commander by a particular time to relate with other available information and intelligence in order to assist in reaching a logical decision. Also called EEIs. (Approved for inclusion in the next edition of JP 1-02.)

estimate. 1. An analysis of a foreign situation, development, or trend that identifies its major elements, interprets the significance, and appraises the future possibilities and the prospective results of the various actions that might be taken. 2. An appraisal of the capabilities, vulnerabilities, and potential courses of action of a foreign nation or combination of nations in consequence of a specific national plan, policy, decision, or contemplated course of action. 3. An analysis of an actual or contemplated clandestine operation in relation to the situation in which it is or would be conducted in order to identify and appraise such factors as available as well as needed assets and potential obstacles, accomplishments, and consequences. See also intelligence estimate. (JP 1-02)

evaluation and feedback. In intelligence usage, continuous assessment of intelligence operations throughout the intelligence process to ensure that the commander's intelligence requirements are being met. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

force protection. Actions taken to prevent or mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information. These actions conserve the force's fighting potential so it can be applied at the decisive time and place and incorporate the coordinated and synchronized offensive and defensive measures to enable the effective employment of the joint force while degrading opportunities for the enemy. Force protection does not include actions to defeat the enemy or protect against accidents, weather, or disease. Also called FP. (JP 1-02)

foreign instrumentation signals intelligence. Technical information and intelligence derived from the intercept of foreign electromagnetic emissions associated with the testing and operational deployment of non-US aerospace, surface, and subsurface systems. Foreign instrumentation signals intelligence is a subcategory of signals intelligence. Foreign instrumentation signals include but are not limited to telemetry, beaconry, electronic interrogators, and video data links. Also called FISINT. See also signals intelligence. (JP 1-02)

foreign intelligence. Intelligence relating to capabilities, intentions, and activities of foreign powers, organizations, or persons (not including counterintelligence), except for information on international terrorist activities. (JP 1-02)

fusion. In intelligence usage, the process of examining all sources of intelligence and information to derive a complete assessment of activity. (JP 1-02)

general military intelligence. Intelligence concerning the (1) military capabilities of foreign countries or organizations or (2) topics affecting potential US or multinational military operations, relating to the following subjects: armed forces capabilities, including order of battle, organization, training, tactics, doctrine, strategy, and other factors bearing on military strength and effectiveness; area and terrain intelligence, including urban areas, coasts and landing beaches, and meteorological, oceanographic, and geological intelligence; transportation in all modes; military materiel production and support industries; military and civilian command, control, communications, computers, and intelligence systems; military economics, including foreign military assistance; insurgency and terrorism; military-political-sociological intelligence; location, identification, and description of military-related installations; government control; escape and evasion; and threats and forecasts. (Excludes scientific and technical intelligence.) Also called GMI. (JP 1-02)

geospatial information and services. The concept for collection, information extraction, storage, dissemination, and exploitation of geodetic, geomagnetic, imagery (both commercial and national source), gravimetric, aeronautical, topographic, hydrographic, littoral, cultural, and toponymic data accurately referenced to a precise location on the earth's surface. These

data are used for military planning, training, and operations including navigation, mission planning, mission rehearsal, modeling, simulation and precise targeting. Geospatial information provides the basic framework for battlespace visualization. It is information produced by multiple sources to common interoperable data standards. It may be presented in the form of printed maps, charts, and publications; in digital simulation and modeling databases; in photographic form; or in the form of digitized maps and charts or attributed centerline data. Geospatial services include tools that enable users to access and manipulate data, and also includes instruction, training, laboratory support, and guidance for the use of geospatial data. Also called GI&S. (JP 1-02)

geospatial intelligence. The analysis and exploitation of imagery, imagery intelligence, and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. (This term and its definition are applicable only in the context of this publication and cannot be referenced outside this publication.)

Global Command and Control System. Highly mobile, deployable command and control system supporting forces for joint and multinational operations across the range of military operations, any time and anywhere in the world with compatible, interoperable, and integrated command, control, communications, computers, and intelligence systems. Also called GCCS. (JP 1-02)

Global Information Grid. The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The Global Information Grid (GIG) includes all owned and leased communications and computing systems and services, software (including applications), data, security services and other associated services necessary to achieve information superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all Department of Defense (DOD), National Security, and related intelligence community missions and functions (strategic, operational, tactical and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms and deployed sites). The GIG provides interfaces to coalition, allied, and non-DOD users and systems. Also called GIG. (JP 1-02)

human intelligence. A category of intelligence derived from information collected and provided by human sources. Also called HUMINT. (JP 1-02)

imagery intelligence. 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. Also called IMINT. (JP 1-02)

indications and warning. Those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to the United States or allied and/or coalition military, political, or economic interests or to US

citizens abroad. It includes forewarning of enemy actions or intentions; the imminence of hostilities; insurgency; nuclear/nonnuclear attack on the United States, its overseas forces, or allied and/or coalition nations; hostile reactions to United States reconnaissance activities; terrorists' attacks; and other similar events. Also called I&W. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

indications (intelligence). Information in various degrees of evaluation, all of which bear on the intention of a potential enemy to adopt or reject a course of action. (JP 1-02)

information operations. Actions taken to affect adversary information and information systems while defending one's own information and information systems. Also called IO. (JP 1-02)

information requirements. Those items of information regarding the adversary and the environment that need to be collected and processed in order to meet the intelligence requirements of a commander. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

information superiority. That degree of dominance in the information domain which permits the conduct of operations without effective opposition. (JP 1-02)

intelligence. 1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. 2. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. (JP 1-02)

intelligence discipline. A well defined area of intelligence collection, processing, exploitation, and reporting using a specific category of technical or human resources. There are seven major disciplines: human intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, open-source intelligence, technical intelligence, and counterintelligence. See also counterintelligence; human intelligence; imagery intelligence; measurement and signature intelligence; open-source intelligence; signals intelligence; and technical intelligence. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

intelligence estimate. The appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to the enemy or potential enemy and the order of probability of their adoption. (JP 1-02)

intelligence federation. A formal agreement in which a combatant command joint intelligence center receives preplanned intelligence support from other joint intelligence centers, Service intelligence organizations, Reserve organizations, and national agencies during crisis or contingency operations.

(This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

intelligence operations. The variety of intelligence and counterintelligence tasks that are carried out by various intelligence organizations and activities within the intelligence process. Intelligence operations include planning and direction, collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

intelligence preparation of the battlespace. An analytical methodology employed to reduce uncertainties concerning the enemy, environment, and terrain for all types of operations. Intelligence preparation of the battlespace builds an extensive database for each potential area in which a unit may be required to operate. The database is then analyzed in detail to determine the impact of the enemy, environment, and terrain on operations and presents it in graphic form. Intelligence preparation of the battlespace is a continuing process. Also called IPB. (JP 1-02)

intelligence process. The process by which information is converted into intelligence and made available to users. The process consists of six interrelated intelligence operations: planning and direction, collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback. (This term and its definition modify the existing term "intelligence cycle" and its definition and are approved for inclusion in the next edition of JP 1-02.)

intelligence-related activities. Those activities outside the consolidated defense intelligence program that: respond to operational commanders' tasking for time-sensitive information on foreign entities; respond to national intelligence community tasking of systems whose primary mission is support to operating forces; train personnel for intelligence duties; provide an intelligence reserve; or are devoted to research and development of intelligence or related capabilities. (Specifically excluded are programs that are so closely integrated with a weapon system that their primary function is to provide immediate-use targeting data.) (JP 1-02)

intelligence requirement. 1. Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence. 2. A requirement for intelligence to fill a gap in the command's knowledge or understanding of the battlespace or threat forces. (JP 1-02)

intelligence source. The means or system that can be used to observe and record information relating to the condition, situation, or activities of a targeted location, organization, or individual. An intelligence source can be people, documents, equipment, or technical sensors. (JP 1-02)

intelligence, surveillance, and reconnaissance. An activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems

in direct support of current and future operations. This is an integrated intelligence and operations function. Also called ISR. (Approved for inclusion in the next edition of JP 1-02.)

intelligence, surveillance, and reconnaissance visualization. The capability to graphically display the current and future locations of intelligence, surveillance, and reconnaissance sensors, their projected platform tracks, vulnerability to threat capabilities and meteorological and oceanographic phenomena, fields of regard, tasked collection targets, and products to provide a basis for dynamic re-tasking and time-sensitive decision making. Also called ISR visualization. (Approved for inclusion in the next edition of JP 1-02.)

intelligence system. Any formal or informal system to manage data gathering, to obtain and process the data, to interpret the data, and to provide reasoned judgments to decision makers as a basis for action. The term is not limited to intelligence organizations or services but includes any system, in all its parts, that accomplishes the listed tasks. (JP 1-02)

interoperability. 1. The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together. 2. (DOD only) The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to specific cases. (JP 1-02)

interpretation. A part of the analysis and production phase in the intelligence process in which the significance of information is judged in relation to the current body of knowledge. See also intelligence process. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

J-2X. A J-2 staff element normally associated with a deployed joint force, consisting of the human intelligence operations cell and the task force counterintelligence coordinating authority. The J-2X is responsible for coordination and deconfliction of all human source-related activity. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

joint captured materiel exploitation center. A physical location for deriving intelligence information from captured enemy materiel. It is normally subordinate to the joint force/J-2. Also called JCMEC. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

joint deployable intelligence support system. A transportable workstation and communications suite that electronically extends a joint intelligence center to a joint task force or other tactical user. Also called JDISS. (JP 1-02)

joint doctrine. Fundamental principles that guide the employment of forces of two or more Military Departments in coordinated action toward a common objective. It is authoritative; as such, joint

doctrine will be followed except when, in the judgment of the commander, exceptional circumstances dictate otherwise. It will be promulgated by or for the Chairman of the Joint Chiefs of Staff, in coordination with the combatant commands and Services. (JP 1-02)

joint document exploitation center. A physical location for deriving intelligence information from captured adversary documents inclusing all forms of electronic data and other forms of stored textual and graphic information. It is normally subordinate to the joint force/J-2. Also called JDEC. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

joint force. A general term applied to a force composed of significant elements, assigned or attached, of two or more Military Departments, operating under a single joint force commander. (JP 1-02)

joint intelligence architecture. A dynamic, flexible structure that consists of the National Military Joint Intelligence Center, the theater joint intelligence centers or joint intelligence center equivalents, and subordinate joint force joint intelligence support elements. This architecture encompasses automated data processing equipment capabilities, communications and information requirements, and responsibilities to provide national, geographic combatant, operational, and tactical commanders with the full range of intelligence required for planning and conducting operations. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

joint intelligence center. The intelligence center of the combatant command headquarters. The joint intelligence center is responsible for providing and producing the intelligence required to support the combatant commander and staff, components, subordinate joint forces and elements, and the national intelligence community. Also called JIC. (JP 1-02)

joint intelligence preparation of the battlespace. The analytical process used by joint intelligence organizations to produce intelligence assessments, estimates, and other intelligence products in support of the joint force commander's decisionmaking process. It is a continuous process that includes defining the total battlespace environment; describing the battlespace's effects; evaluating the adversary; and determining and describing adversary potential courses of actions. The process is used to analyze the air, land, sea, space, electromagnetic, cyberspace, and human dimensions of the environment and to determine an opponent's capabilities to operate in each. Joint intelligence preparation of the battlespace products are used by the joint force and component command staffs in preparing their estimates and are also applied during the analysis and selection of friendly courses of action. Also called JIPB. (JP 1-02)

joint intelligence support element. A subordinate joint force element whose focus is on intelligence support for joint operations, providing the joint force commander, joint staff, and components with the complete air, space, ground, and maritime adversary situation. Also called JISE. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

joint interrogation and debriefing center. A physical location for the exploitation of intelligence information from enemy prisoners of war and other nonprisoner sources. It is normally subordinate to the joint force/J-2. Also called JIDC. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

joint interrogation operations. 1. Activities conducted by a joint or interagency organization to extract information for intelligence purposes from enemy prisoners of war, dislocated civilians, enemy combatants, or other uncategorized detainees. 2. Activities conducted in support of law enforcement efforts to adjudicate enemy combatants who are believed to have committed crimes against US persons or property. Also called JIO. (Approved for inclusion in the next edition of JP 1-02.)

Joint Worldwide Intelligence Communications System. The sensitive, compartmented information portion of the Defense Information System Network. It incorporates advanced networking technologies that permit point-to-point or multipoint information exchange involving voice, text, graphics, data, and video teleconferencing. Also called JWICS. (JP 1-02)

Measurement and Signature Intelligence Requirements System. A system for the management of theater and national measurement and signature intelligence (MASINT) collection requirements. It provides automated tools for users in support of submission, review, and validation of MASINT nominations of requirements to be tasked for national and Department of Defense MASINT collection, production, and exploitation resources. Also called MRS. (Approved for inclusion in the next edition of JP 1-02.)

measurement and signature intelligence. Technically derived intelligence that detects, locates, tracks, identifies, and describes the unique characteristics of fixed and dynamic target sources. Measurement and signature intelligence capabilities include radar, laser, optical, infrared, acoustic, nuclear radiation, radio frequency, spectroradiometric, and seismic sensing systems as well as gas, liquid, and solid materials sampling and analysis. Also called MASINT. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

medical intelligence. That category of intelligence resulting from collection, evaluation, analysis, and interpretation of foreign medical, bio-scientific, and environmental information which is of interest to strategic planning and to military medical planning and operations for the conservation of the fighting strength of friendly forces and the formation of assessments of foreign medical capabilities in both military and civilian sectors. Also called MEDINT. (JP 1-02)

military intelligence. Intelligence on any foreign military or military-related situation or activity which is significant to military policymaking or the planning and conduct of military operations and activities. Also called MI. (JP 1-02)

Military Intelligence Board. A decisionmaking forum which formulates Defense intelligence policy and programming priorities. The Military Intelligence Board, chaired by the Director, Defense Intelligence Agency, who is dual-hatted as Director of Military Intelligence, consists of senior military and civilian intelligence officials of each Service, US Coast Guard, each Combat Support Agency, the Joint Staff/J-2/J-6, Deputy Assistant Secretary of Defense (Intelligence), Intelligence Program Support Group, DIA's Directorates for Intelligence Production, Intelligence Operations, and Information and Services, and the combatant command J-2s. Also called MIB. (JP 1-02)

Modernized Integrated Database. The national level repository for the general military intelligence available to the entire Department of Defense Intelligence Information System community and, through Global Command and Control System integrated imagery and intelligence, to tactical units. This data is maintained and updated by the Defense Intelligence Agency. Commands and Services are delegated responsibility to maintain their portion of the database. Also called MIDB. (JP 1-02)

munitions effectiveness assessment. Conducted concurrently and interactively with battle damage assessment, the assessment of the military force applied in terms of the weapon system and munitions effectiveness to determine and recommend any required changes to the methodology, tactics, weapon system, munitions, fusing, and/or weapon delivery parameters to increase force effectiveness. Munitions effectiveness assessment is primarily the responsibility of operations with required inputs and coordination from the intelligence community. Also called MEA. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

national intelligence. Integrated departmental intelligence that 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. (JP 1-02)

national intelligence estimate. A strategic estimate of the capabilities, vulnerabilities, and probable courses of action of foreign nations produced at the national level as a composite of the views of the intelligence community. Also called NIE. (JP 1-02)

national intelligence support team. A nationally sourced team composed of intelligence and communications experts from either Defense Intelligence Agency, Central Intelligence Agency, National Security Agency, or any combination of these agencies. Also called NIST. (JP 1-02)

National Military Joint Intelligence Center. The national-level focal point for all defense intelligence activities in support of joint operations. Also called NMJIC. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

open-source intelligence. Information of potential intelligence value that is available to the general public. Also called OSINT. (JP 1-02)

operational intelligence. Intelligence that is required for planning and conducting campaigns and major operations to accomplish strategic objectives within theaters or operational areas. (JP 1-02)

operation order. A directive issued by a commander to subordinate commanders for the purpose of effecting the coordinated execution of an operation. Also called OPORD. (JP 1-02)

operation plan. Any plan, except for the Single Integrated Operational Plan, for the conduct of military operations. Plans are prepared by combatant commanders in response to requirements established by the Chairman of the Joint Chiefs of Staff and by commanders of subordinate commands in response to requirements tasked by the establishing unified commander. Operation plans are prepared either in a complete format (OPLAN) or as a concept plan (CONPLAN). The CONPLAN can be published with or without a time-phased force and deployment data (TPFDD) file. a. OPLAN — An operation plan for the conduct of joint operations that can be used as a basis for development of an operation order (OPORD). An OPLAN identifies the forces and supplies required to execute the combatant commander's strategic concept and a movement schedule of these resources to the theater of operations. The forces and supplies are identified in TPFDD files. OPLANs will include all phases of the tasked operation. The plan is prepared with the appropriate annexes, appendixes, and TPFDD files as described in the Joint Operation Planning and Execution System manuals containing planning policies, procedures, and formats. Also called OPLAN. b. CONPLAN — An operation plan in an abbreviated format that would require considerable expansion or alteration to convert it into an OPLAN or OPORD. A CONPLAN contains the combatant commander's strategic concept and those annexes and appendixes deemed necessary by the combatant commander to complete planning. Generally, detailed support requirements are not calculated and TPFDD files are not prepared. Also called CONPLAN. c. CONPLAN with TPFDD — A CONPLAN with TPFDD is the same as a CONPLAN except that it requires more detailed planning for phased deployment of forces. Also called CONPLAN. (JP 1-02)

persistent surveillance. A collection strategy that emphasizes the ability of some collection systems to linger on demand in an area to detect, locate, characterize, identify, track, target, and possibly provide battle damage assessment and re-targeting in near or real-time. Persistent surveillance facilitates the formulation and execution of preemptive activities to deter or forestall anticipated adversary courses of action. (Approved for inclusion in the next edition of JP 1-02.)

planning and direction. In intelligence usage, the determination of intelligence requirements, development of appropriate intelligence architecture, preparation of a collection plan, and issuance of orders and requests to information collection agencies. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

priority intelligence requirements. Those intelligence requirements for which a commander has an anticipated and stated priority in the task of planning and decision making. Also called PIRs. (JP 1-02)

processing and exploitation. In intelligence usage, the conversion of collected information into forms suitable to the production of intelligence. (Approved for inclusion in the next edition of JP 1-02.)

psychological operations. Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. Also called PSYOP. (JP 1-02)

reconnaissance. A mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area. Also called RECON. (JP 1-02)

request for information. 1. Any specific time-sensitive ad hoc requirement for intelligence information or products to support an ongoing crisis or operation not necessarily related to standing requirements or scheduled intelligence production. A request for information can be initiated to respond to operational requirements and will be validated in accordance with the theater command's procedures. 2. The National Security Agency/Central Security Service uses this term to state ad hoc signals intelligence requirements. Also called RFI. (JP 1-02)

requirements management system. A system for the management of theater and national imagery collection requirements that provides automated tools for users in support of submission, review, and validation of imagery nominations as requirements to be tasked on national or Department of Defense imagery collection, production, and exploitation resources. Also called RMS. (JP 1-02)

scientific and technical intelligence. The product resulting from the collection, evaluation, analysis, and interpretation of foreign scientific and technical information that covers: a. foreign developments in basic and applied research and in applied engineering techniques; and b. scientific and technical characteristics, capabilities, and limitations of all foreign military systems, weapons, weapon systems, and materiel; the research and development related thereto; and the production methods employed for their manufacture. Also called S&TI. (JP 1-02)

SECRET Internet Protocol Router Network. Worldwide SECRET level packet switch network that uses high-speed internet protocol routers and high-capacity Defense Information Systems Network circuitry. Also called SIPRNET. (JP 1-02)

sensitive compartmented information. All information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentation have been or will be formally established. (These controls are over and above the provisions of DOD 5200.1-R, Information Security Program Regulation.) Also called SCI. (JP 1-02)

sensitive compartmented information facility. An accredited area, room, group of rooms, or installation where sensitive compartmented information (SCI) may be stored, used, discussed, and/or electronically processed. Sensitive compartmented information facility (SCIF) procedural and physical measures prevent the free access of persons unless they have been formally indoctrinated for the particular SCI authorized for use or storage within the SCIF. Also called SCIF. (JP 1-02)

SIGINT operational tasking authority. A military commander's authority to operationally direct and levy signals intelligence (SIGINT) requirements on designated SIGINT resources; includes authority to deploy and redeploy all or part of the SIGINT resources for which SIGINT operational tasking authority has been delegated. Also called SOTA. (JP 1-02)

signals intelligence. 1. A category of intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted. 2. Intelligence derived from communications, electronic, and foreign instrumentation signals. Also called SIGINT. (JP 1-02)

strategic intelligence. Intelligence that is required for the formulation of strategy, policy, and military plans and operations at national and theater levels. (JP 1-02)

surveillance. The systematic observation of aerospace, surface, or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means. (JP 1-02)

tactical intelligence. Intelligence that is required for planning and conducting tactical operations. Also called TACINTEL. (JP 1-02)

targeting. The process of selecting and prioritizing targets and matching the appropriate response to them, taking account of operational requirements and capabilities. (JP 1-02)

tear line. A physical line on an intelligence message or document separating categories of information that have been approved for foreign disclosure and release. Normally, the intelligence below the tear line is that which has been previously cleared for disclosure or release. (JP 1-02)

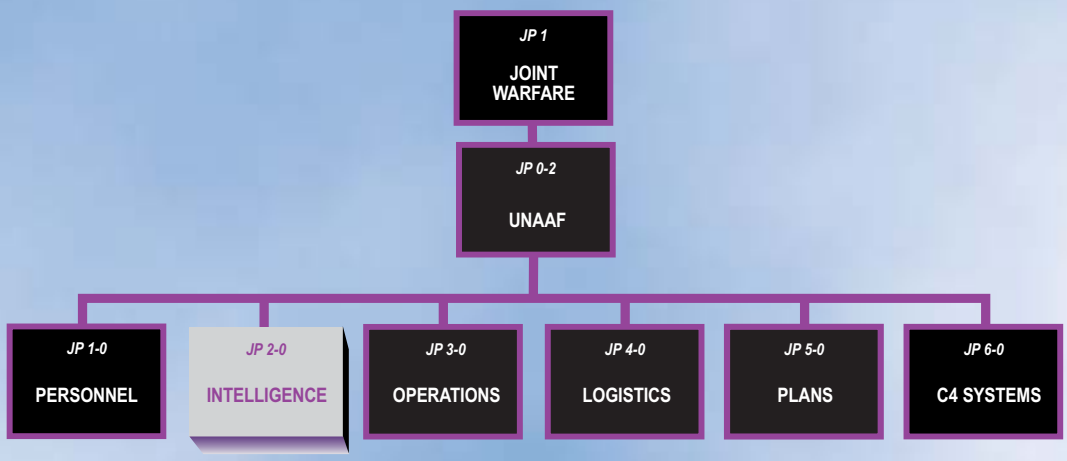
technical intelligence. Intelligence derived from exploitation of foreign material, produced for strategic, operational, and tactical level commanders. Technical intelligence begins when an individual service member finds something new on the battlefield and takes the proper steps to report it. The item is then exploited at succeedingly higher levels until a countermeasure is produced to neutralize the adversary's technological advantage. Also called TECHINT. (JP 1-02)

threat warning. The urgent communication and acknowledgement of time-critical information essential for the preservation of life and/or vital resources. (Approved for inclusion in the next edition of JP 1-02.)

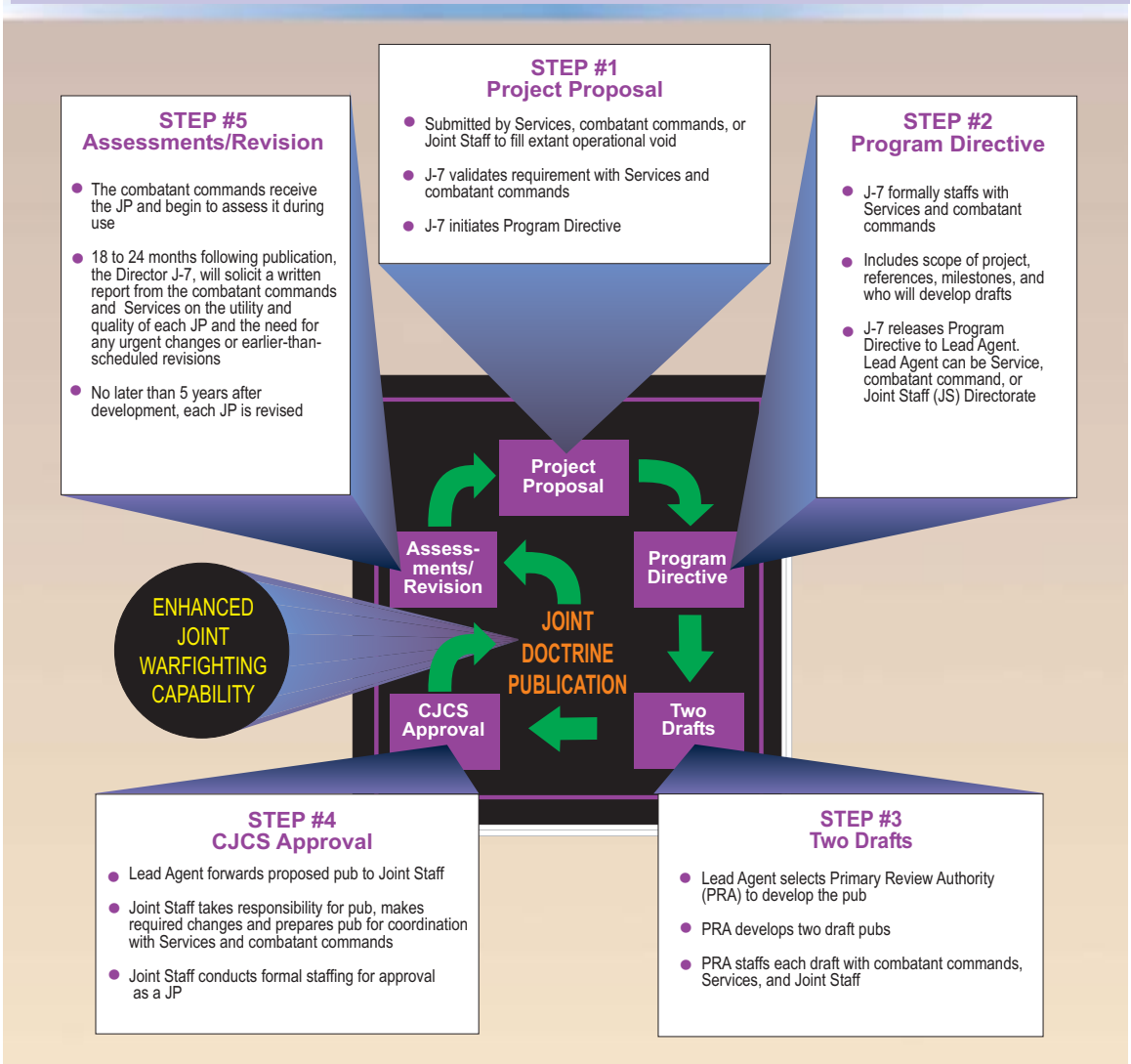
validation. 1. A process associated with the collection and production of intelligence that confirms that an intelligence collection or production requirement is sufficiently important to justify the dedication of intelligence resources, does not duplicate an existing requirement, and has not been previously satisfied. 2. In computer modeling and simulation, the process of determining the degree to which a model or simulation is an accurate representation of the real world from the perspective of the intended uses of the model or simulation. 3. Execution procedure used by combatant command components, supporting combatant commanders, and providing organizations to confirm to the supported commander and US Transportation Command that all the information records in a time-phased force and deployment data not only are error free for automation purposes, but also accurately reflect the current status, attributes, and availability of units and requirements. Unit readiness, movement dates, passengers, and cargo details should be confirmed with the unit before validation occurs. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

weapons of mass destruction. Weapons that are capable of a high order of destruction and/or of being used in such a manner as to destroy large numbers of people. Weapons of mass destruction can be high explosives or nuclear, biological, chemical, and radiological weapons, but exclude the means of transporting or propelling the weapon where such means is a separable and divisible part of the weapon. Also called WMD. (JP 1-02)

JOINT DOCTRINE PUBLICATIONS HIERARCHY



All joint doctrine and tactics, techniques, and procedures are organized into a comprehensive hierarchy as shown in the chart above. **Joint Publication (JP) 2-01** is in the **Intelligence** series of joint doctrine publications. The diagram below illustrates an overview of the development process:




JOINT
CHIEFS OF STAFF